Cisco IOS Security Command Reference: Commands M to R

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

mab through mime-type

mab

To enable MAC-based authentication on a port, use the **mab** command in interface configuration or template configuration mode. To disable MAC-based authentication, use the **no** form of this command.

mab [eap]

no mab

Syntax Description

eap	(Optional) Configures the port to use Extensible Authentication Protocol (EAP).

Command Default

MAC-based authentication is not enabled.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

Use the **mab** command to enable MAC-based authentication on a port. To enable EAP on the port, use the **mab eap** command.

Note If you are unsure whether MAB or MAB EAP is enabled or disabled on the switched port, use the **default mab**or **default mab eap** commands in interface configuration mode to configure MAB or MAB EAP to its default.

Examples

The following example shows how to configure MAC-based authorization on a Gigabit Ethernet port:

```
Switch(config)# interface GigabitEthernet6/2
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# mab
Switch(config-if)# end
```

The following example shows how to configure MAC-based authorization on an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# mab
Device(config-template)# end
```

Related Commands

Command	Description
show mab	Displays information about MAB.

mac access-group

To use a MAC access control list (ACL) to control the reception of incoming traffic on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, an 802.1Q-in-Q stacked VLAN subinterface, use the **macaccess-group**command in interface or subinterface configuration mode. To remove a MAC ACL, use the **no** form of this command.

mac access-group *access-list-number* **in**

no mac access-group *access-list-number* **in**

Syntax Description

access-list-number	Number of a MAC ACL to apply to an interface or subinterface (as specified by a **access-list(MAC)** command). This is a decimal number from 700 to 799.
in	Filters on inbound packets.

Command Default

No access list is applied to the interface or subinterface.

Command Modes

Interface configuration (config-if) Subinterface configuration (config-subif)

Command History

Release	Modification
12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

MAC ACLs are applied on incoming traffic on Gigabit Ethernet interfaces and VLAN subinterfaces. After a networking device receives a packet, the Cisco IOS software checks the source MAC address of the Gigabit Ethernet, 802.1Q VLAN, or 802.1Q-in-Q packet against the access list. If the MAC access list permits the address, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified MAC ACL does not exist on the interface or subinterface, all packets are passed.

On Catalyst 6500 series switches, this command is supported on Layer 2 ports only.

Note The **macaccess-group**command is supported on a VLAN subinterface only if a VLAN is already configured on the subinterface.

Examples

The following example applies MAC ACL 101 on incoming traffic received on Gigabit Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# mac access-group 101 in
```

Related Commands

Command	Description
access-list (MAC)	Defines a MAC ACL.
clear mac access-list counters	Clears the counters of a MAC ACL.
ip access-group	Configures an IP access list to be used for packets transmitted from the asynchronous host.
show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.
show mac access-list	Displays the contents of one or all MAC ACLs.

mac-address (RITE)

To specify the Ethernet address of the destination host, use the **mac-address** command in router IP traffic export (RITE) configuration mode. To change the MAC address of the destination host, use the **no** form of this command.

mac-address *H.H.H*

nomac-address *H.H.H*

Syntax Description

H.H.H	48-bit MAC address.

Command Default

A destination host is not known.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

The **mac-address** command, which is used to specify the destination host that is receiving the exported traffic, is part of suite of RITE configuration mode commands that are used to control various attributes for both incoming and outgoing IP traffic export.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control lists (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
```

```
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

managed-config-flag

To verify the advertised managed address configuration parameter, use the **managed-config-flag** command in RA guard policy configuration mode.

managed-config-flag {**on**| **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **managed-config-flag** command enables verification of the advertised managed address configuration parameter (or "M" flag). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables M flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# managed-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

map type

To define the mapping of an attribute in the Lightweight Directory Access Protocol (LDAP) server, use the **map type**command in attribute-map configuration mode. To remove the attribute maps, use the **no** form of this command.

map type *ldap-attr-type aaa-attr-type* [**format** *dn-to-string*]

no map type *ldap-attr-type aaa-attr-type* [**format** *dn-to-string*]

Syntax Description

ldap-attr-type	LDAP attribute type.
aaa-attr-type	Authentication, Authorization, and Accounting (AAA) attribute type.
format	(Optional) Specifies the format conversion for attribute.
dn-to-string	(Optional) Converts the distinguished name (DN) to string format.

Command Default

No mapping types are defined.

Command Modes

Attribute-map configuration (config-attr-map)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

To use the attribute mapping features, you need to understand the Cisco AAA attribute names and values as well as the LDAP servers user-defined attribute names and values.

Examples

The following example shows how to map the user-defined attribute named department to the AAA attribute named element-req-qos in an LDAP server.

```
Router(config)# ldap attribute-map att_map_1
Router(config-attribute-map)# map type department element-req-qos format dn-to-string
Router(config-attribute-map)# exit
```

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

mask (policy-map)

To explicitly mask specified SMTP commands or the parameters returned by the server in response to an EHLO command, use the **mask** command in global configuration mode. To remove this filter from the configuration, use the **no** form of this command:

mask

no mask

Command Default

The command-level default is not enabled.

Command Modes

Policy-map configuration mode.

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Using the **mask** command applies to certain 'match' command filters like the **match cmd command and the verb keyword**. Validations are performed to make this check and the configuration is not be accepted in case of invalid combinations.

Examples

The following example shows how the **mask** command is used with the **match cmd command and verb** keyword to prevent ESMTP inspection:

```
class-map type inspect smtp c1
 match cmd verb EHLO
policy-map type inspect smtp c1
 class type inspect smtp c1
  mask
```

Related Commands

Command	Description
match cmd	Specifies a value that limits the length of the ESMTP command line or the ESMTP command line verb used to thwart denial of service (DoS) attacks

mask-urls

To obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers, use the **mask-urls** command in webvpn group policy configuration mode. To remove the masking, use the **no** form of this command.

mask-urls

no mask-urls

Syntax Description

This command has no arguments or keywords.

Command Default

Sensitive portions of an enterprise URL are not masked.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is configured in group configuration only.

Examples

The following example shows that URL obfuscation (masking) has been configured for policy group “GP”:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group GP
Router(config-webvpn-group)# mask-urls
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

master (IKEv2 cluster)

To define the settings for the master gateway in a Hot Standby Router Protocol (HSRP) cluster, use the **master** command in IKEv2 cluster configuration mode. To restore the default settings, use the **no** form of this command.

master {**overload-limit** *percent* | **weight** {**crypto-load** *weight-number* | **system-load** *weight-number*}}

no master {**overload-limit** | **weight** {**crypto-load** | **system-load**}}

Syntax Description

overload-limit *percent*	Specifies the threshold limit of a cluster. The range is from 50 to 99. The default is 99.
weight	Specifies the weight of a load attribute.
crypto-load *weight-number*	Specifies the Internet Key Exchange (IKE) and IPsec weight limit. The range is from 0 to 100. The default is 100.
system-load *weight-number*	Specifies the CPU and memory weight limit. The range is from 0 to 100. The default is 100.

Command Default

The default master settings are used.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **master** command.

The load limit helps to decide if a device is busy and ignore it for redirection by specifying the weight of an attribute.

Examples

The following example show how to set the crypto load setting to 10 for the HSRP master gateway:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# master weight crypto-load 10
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

match (gtp)

To configure the classification criteria for inspect-type class map for General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **match** command in class-map configuration mode. To disable the classification criteria, use the **no** form of this command.

match {**apn regex** *parameter-map-name*| **mcc** *country-code* **mnc** *network-code*| **message-id** *id*| **message-length min** *min-length* **max** *max-length*| **version** *number*}

no match {**apn**| **mcc** *country-code* **mnc** *network-code*| **message-id** *id*| **message-length**| **version** *number*}

Syntax Description

apn	Configures filtering for the GTP Access Point Name (APN).
regex	Specifies the APN address for the GNU regular expression (regex) matching library.
parameter-map-name	Name of the APN regex parameter map.
mcc	Configures filtering for a valid Mobile Country Code (MCC).
country-code	Mobile country code. The range is from 0 to 999.
mnc	Configures filtering for Mobile Network Code (MNC).
network-code	Mobile network code. The range is from 0 to 999.
message-id *id*	Configures filtering for the GTP message ID. The range is from 1 to 255.
message-length	Configures filtering for the GTP message length.
min	Specifies the minimum length of the GTP message.
min-length	Minimum length, in bytes, of the GTP message. The range is from 1 to 65536.
max	Specifies the maximum length of the GTP message.
max-length	Maximum length, in bytes, of the GTP message. The range is from 1 to 65536.
version *number*	Configures filtering for the GTP version. Accepted values are 0 and 1.

Command Default

No classification criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The **mcc** *country-code* and **mnc** *network-code* keyword-argument combinations are used for International Mobile Subscriber Identity (IMSI) prefix filtering, where the country code contains three digits and the network code contains two- or three-digit values. The **message-length** keyword allows you to filter packets that do not meet the configured maximum and minimum length values. This length is the sum of the GTP header and the rest of the message. For example, the payload of the UDP packet. The **apn** keyword allows you to activate action on GTP messages with the specified APN. The **message-id** keyword allows you to activate action on specific GTP messages. The **version** keyword allows you to activate action on GTP messages with the specified version.

Examples

The following example shows how to configure match criteria for a message with a minimum length of 300 bytes and a maximum length of 500 bytes for inspect-type class map for GTPv0.

```
Router(config)# class-map type inspect gtpv0 LAYER7_CLASS_MAP
Router(config-cmap)# match message-length min 300 max 500
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type class map.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in QoS class-map configuration or policy inline configuration mode. To remove the ACL match criteria from a class map, use the **no** form of this command.

match access-group {*access-group*| **name** *access-group-name*}

no match {*access-group*| **name** *access-group-name*}

Syntax Description

access-group	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The range is from 1 to 2699.
name *access-group-name*	Specifies a named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The name can be up to 40 alphanumeric characters.

Command Default

No match criteria are configured.

Command Modes

QoS class-map configuration (config-cmap)

Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was modified. This command was enhanced to include matching of access lists on the Cisco 10000 series routers.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(6)T	This command was modified. This command was enhanced to support the zone-based policy firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Release	Modification
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

Usage Guidelines

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

A traffic rate is generated for packets that match an access group. In zone-based policy firewalls, only the first packet that creates a session matches the configured policy. Subsequent packets in the flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

Zone-based policy firewalls support only the **match access-group**, **match class-map**, and **match protocol** commands. If you specify more than one **match** command in a class map, only the last command that you specified will be applied to the class map. The last **match** command overrides the previously entered **match** commands.

The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the **log** keyword of the **access-list** command are not supported when you configure the match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

When this command is configured in Cisco IOS Release 15.0(1)M and later releases, the firewall inspects only Layer 4 policy maps. In releases prior to Cisco IOS Release 15.0(1)M, the firewall inspects both Layer 4 and Layer 7 policy maps.

For class-based weighted fair queueing (CBWFQ), you can define traffic classes based on the match criteria that include ACLs, experimental (EXP) field values, input interfaces, protocols, and quality of service (QoS) labels. Packets that satisfy the match criteria for a class constitute the traffic for that class.

Note In zone-based policy firewalls, this command is not applicable for CBWFQ.

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration modes in which you can issue this command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

To use the **match access-group** command, you must configure the **service-policy type performance-monitor inline** command.

Supported Platforms Other than Cisco 10000 Series Routers

To use the **match access-group** command, you must configure the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the **log** keyword of the **access-list** command are not supported when you configure the match criteria.

Cisco ASR 1000 Series Aggregation Services Routers

Cisco ASR 1000 Series Routers do not support more than 16 match statements per class map. An interface with more than 16 match statements rejects the service policy.

Examples

The following example shows how to specify a class map named acl144 and to configure the ACL numbered 144 to be used as the match criterion for that class:

```
Device(config)# class-map acl144
Device(config-cmap)# match access-group 144
```

The following example shows how to define a class map named c1 and configure the ACL numbered 144 to be used as the match criterion for that class:

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 144
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to configure a service policy for the Performance Monitor in policy inline configuration mode. The policy specifies that packets traversing Ethernet interface 0/0 must match ACL144.

```
Device(config)# interface ethernet 0/0
Device(config-if)# service-policy type performance-monitor inline input
Device(config-if-spolicy-inline)# match access-group name ACL144
Device(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.

Command	Description
access-list (IP standard)	Defines a standard IP access list.
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match class-map	Uses a traffic class as a classification policy.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.

match address (GDOI local server)

To specify an IP extended access list for a Group Domain of Interpretation (GDOI) registration, use the **match address** command in GDOI SA IPsec configuration mode. To disable the access list, use the **no** form of this command.

match address {**ipv4| ipv6**} {*access-list-number*| *access-list-name*}

no match address {**ipv4| ipv6**} {*access-list-number*| *access-list-name*}

Syntax Description

ipv4	Specifies that IPv4 packets should be matched.
ipv6	Specifies that IPv6 packets should be matched.
access-list-number | *access-list-name*	Access list number or name. This value should match the access list number or name of the extended access list that is being matched. IPv6 configurations must use named access lists. The range is 100 through 199 or 2000 through 2699 for an expanded range.

Command Default

No access lists are matched to the GDOI entry.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.2(3)T	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

If you attempt to assign an IPv6 group with IPv4 policies, an error message appears indicating that the access list name is invalid or that the list already exists but is the wrong type.

Examples

The following example shows how to specify an IP extended access list named 102 for IPv4 traffic. This example uses an identity number (rather than an identity address) and a profile named gdoi-p:

```
Router# enable
Router# configure terminal
Router(config)# crypto gdoi group gdoigroupname
Router(config-gdoi-group)# identity number 3333
Router(config-gdoi-group)# server local
```

```
Router(gdoi-local-server)# sa ipsec 1
Router(gdoi-sa-ipsec)# profile gdoi-p
Router(gdoi-sa-ipsec)# match address ipv4 102
```

The following example shows how to specify an IP extended access list named group1_v6 for IPv6 traffic. This example uses a profile named gdoi-p2:

```
Router# enable
Router# configure terminal
Router(config)# crypto gdoi group ipv6 gdoigroupname2
Router(config-gdoi-group)# identity number 3333
Router(config-gdoi-group)# server local
Router(gdoi-local-server)# sa ipsec 1
Router(gdoi-sa-ipsec)# profile gdoi-p2
Router(gdoi-sa-ipsec)# match address ipv6 group1_v6
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

match address (IPSec)

To specify an extended access list for a crypto map entry, use the **match address** command in crypto map configuration mode. To remove the extended access list from a crypto map entry, use the **no** form of this command.

match address [*access-list-id*| *name*]

no match address [*access-list-id*| *name*]

Syntax Description

access-list-id	(Optional) Identifies the extended access list by its name or number. This value should match the *access-list-number* or *name* argument of the extended access list being matched.
name	(Optional) Identifies the named encryption access list. This name should match the *name* argument of the named encryption access list being matched.

Command Default

No access lists are matched to the crypto map entry.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required for all static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use this command to assign an extended access list to a crypto map entry. You also need to define this access list using the **access-list**or **ip access-list extended** commands.

The extended access list specified with this command will be used by IPSec to determine which traffic should be protected by crypto and which traffic does not need crypto protection. (Traffic that is permitted by the access list will be protected. Traffic that is denied by the access list will not be protected in the context of the corresponding crypto map entry.)

Note that the crypto access list is *not* used to determine whether to permit or deny traffic through the interface. An access list applied directly to the interface makes that determination.

The crypto access list specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists specified by the interface's crypto map entries to determine if it should be protected by crypto and if so (if traffic matches a **permit** entry) which crypto policy applies. (If necessary, in the case of static IPSec crypto maps, new security associations are established using the data flow identity as specified in the **permit** entry; in the case of dynamic crypto map entries, if no SA exists, the packet is dropped.) After passing the regular access lists at the interface, inbound traffic is evaluated against the crypto access lists specified by the entries of the interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (In the case of IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

In the case of IPSec, the access list is also used to identify the flow for which the IPSec security associations are established. In the outbound case, the **permit** entry is used as the data flow identity (in general), while in the inbound case the data flow identity specified by the peer must be "permitted" by the crypto access list.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the security associations. (This example is for a static crypto map.)

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.

Command	Description
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

match authentication trustpoint

To specify the trustpoint name that should be used to authenticate the SDP peer's certificate, use the **match authentication trustpoint**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

match authentication trustpoint *trustpoint-name*

no match authentication trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the truspoint name.

Command Default

No trustpoint name is specified for the iPhone deployment.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match authentication trustpoint**command can be used optionally in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

If the trustpoint name is not specified, then the trustpoint configured using the **authentication trustpoint**in tti-registrar configuration mode is used to authenticate the SDP peer's certificate.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match url	Specifies the URL to be associated with the URL profile.
authentication trustpoint	Specifies the trustpoint used to authenticate the SDP petitioner device's existing certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

match body regex

To specify an arbitrary text expression to restrict specified content-types and content encoding types for text and HTML in the "body" of the e-mail, use the **match body regex** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match body regex *parameter-map-name*

no match body regex *parameter-map-name*

Syntax Description

parameter-map-name	Name of a specific traffic pattern specified through the **parameter-map type regex**command.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

The text or HTML pattern is scanned only if the encoding is 7-bit or 8-bit and the encoding is checked before attempting to match the pattern. If the pattern is of another encoding type (For example, base64, zip files etc.), then the pattern cannot be scanned

Note Using this command can impact performance because the complete SMTP connection has to be scanned.

Examples

The following example shows how to configure an SMTP policy to block an e-mail that contains the pattern "*UD-421590*" in the body of an e-mail.

```
parameter-map type regex doc-data
pattern "*UD-421590*"
class-map type inspect smtp c1
match body regex doc-data
policy-map type inspect smtp p1
```

```
class type inspect smtp c1
log
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match certificate

To specify the name of the certificate map used to authorize the peer's certificate, use the **match certificate**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

match certificate *certificate-map*

no match certificate *certificate-map*

Syntax Description

certificate-map	Specifies the certificate map name.

Command Default

No certificate map name is specified for the iPhone deployment.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match certificate**command can be used optionally in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.

Command	Description
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match url	Specifies the URL to be associated with the URL profile.
match authentication trustpoint	Specifies the trustpoint name that should be used to authenticate the SDP peer's certificate in order to deploy Apple iPhones on a corporate network.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

match certificate (ca-trustpoint)

To associate a certificate-based access control list (ACL) that is defined with the **crypto ca certificate map** command, use the **match certificate** command in ca-trustpoint configuration mode. To remove the association, use the **no** form of this command.

match certificate *certificate-map-label* [**allow expired-certificate**| **skip revocation-check**| **skip authorization-check**]

no match certificate *certificate-map-label* [**allow expired-certificate**| **skip revocation-check**| **skip authorization-check**]

Syntax Description

certificate-map-label	Matches the *label* argument specified in a previously defined **crypto ca certificate map** command.
allow expired-certificate	(Optional) Ignores expired certificates. **Note** If this keyword is not configured, the router does not ignore expired certificates.
skip revocation-check	(Optional) Allows a trustpoint to enforce certificate revocation lists (CRLs) except for specific certificates. **Note** If this keyword is not configured, the trustpoint enforces CRLs for all certificates.
skip authorization-check	(Optional) Skips the authentication, authorization, and accounting (AAA) check of a certificate when public key infrastructure (PKI) integration with an AAA server is configured. **Note** If this keyword is not configured and PKI integration with an AAA server is configured, the AAA checking of a certificate is done.

Command Default

If this command is not configured, no default match certificate is configured. Each of the **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords have a default (see the "Syntax Description" section).

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Release	Modification
12.3(4)T	The **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **match certificate**command associates the certificate-based ACL defined with the **crypto ca certificate map** command to the trustpoint. The *certificate-map-label* argument in the **match certificate** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

The certificate map with the label *certificate-map-label* must be defined before it can be used with the **match certificate** subcommand.

A certificate referenced in a **match certificate** command may not be deleted until all references to the certificate map are removed from configured trustpoints (that is, no **match certificate** commands can reference the certificate map being deleted).

When the certificate of a peer has been verified, the certificate-based ACL as specified by the certificate map is checked. If the certificate of the peer matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the certificate of the peer, the certificate of the peer is considered valid.

If the certificate map does not have any attributes defined, the certificate is rejected.

Using the allow expired-certificate Keyword

The **allow expired-certificate** keyword has two purposes:

- If the certificate of a peer has expired, this keyword may be used to "allow" the expired certificate until the peer is able to obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This keyword may be used to allow the certificate of the peer even though your router clock is not set.

Note If Network Time Protocol (NTP) is available only via the IPSec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be "brought up" because the certificate of the hub is not yet valid.

- "Expired" is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end time specified in the certificate.

Using the skip revocation-check Keyword

The type of enforcement provided using the **skip revocation-check** keyword is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. If one spoke communicates directly with another spoke, the CRLs must be checked. However, if the trustpoint is configured to require CRLs, the connection to the hub to retrieve the CRL usually cannot be made because the CRL is available only via the connection hub.

Using the skip authorization-check Keyword

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **skip authorization-check** keyword. For example, if a Virtual Private Network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **skip authorization-check keyword** to skip the certificate check so that the tunnel can be established.

The **skip authorization-check** keyword should be configured after PKI integration with an AAA server is configured.

Examples

The following example shows a certificate-based ACL with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

The following example shows a configuration for a central site using the **allow expired-certificate** keyword. The router at a branch site has an expired certificate named "branch1" and has to establish a tunnel to the central site to renew its certificate.

```
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
 match certificate branch1 allow expired-certificate
```

The following example shows a branch office configuration using the **skip revocation-check** keyword. The trustpoint is being allowed to enforce CRLs except for "central-site" certificates.

```
crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Branch 1
 revocation-check crl
 match certificate central-site skip revocation-check
```

The following example shows a branch office configuration using the **skip authorization-check** keyword. The trustpoint is being allowed to skip AAA checking for the central site.

```
crypto pki trustpoint home-office
 auth list allow_list
 auth user subj commonname
 match certificate central-site skip authorization-check
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match certificate (ca-trustpool)

To enable the use of certificate maps for the public key infrastructure (PKI) trustpool, use the **match certificate** command in ca-trustpool configuration mode. To remove the association, use the **no** form of this command.

match certificate *certificate-map-name* [**allow expired-certificate**| **override** {**cdp directory** *ldap-location*| **ocsp** {*number url*| **trustpool** *name number* **url** *url*}| **sia** *number url*}| **skip** [**revocation-check**| **authorization-check**]]

no match certificate *certificate-map-name* [**allow expired-certificate**| **override** {**cdp directory** *ldap-location*| **ocsp** {*number url*| **trustpool** *name number* **url** *url*}| **sia** *number url*}| **skip** [**revocation-check**| **authorization-check**]]

Syntax Description

certificate-map-name	The certificate map name that is matched.
allow expired-certificate	(Optional) Ignores expired certificates. **Note** If this keyword combination is not configured, the router does not ignore expired certificates.
override	Overrides the online certificate status protocol (OCSP), or SubjectInfoAccess (SIA) attribute fields in a certificate that is in the PKI trustpool.
cdp	Overrides the certificate distribution point (CDP) in a certificate.
directory *ldap-location*	Specifies the CDP in either the http: or ldap: URL, or the Lightweight Directory Access Protocol (LDAP) directory to override in the certificate.
ocsp *number url*	Specifies the OCSP sequence number from 0 to 10000 and URL to override in the certificate.
trustpool *name number* **url** *url*	Overrides the PKI trustpool for verifying the OCSP certificate by specifying the PKI trustpool name, sequence number, and URL.
sia *number url*	Overrides the SIA URL in a certificate by specifying the SIA sequence number and URL.
skip revocation-check	(Optional) Allows the PKI trustpool to enforce certificate revocation lists (CRLs) except for specific certificates. **Note** If this keyword combination is not configured, the PKI trustpool enforces CRLs for all certificates.

skip authorization-check	(Optional) Skips the authentication, authorization, and accounting (AAA) check of a certificate when PKI integration with an AAA server is configured. **Note** If this keyword combination is not configured and PKI integration with an AAA server is configured, the AAA checking of a certificate is done.

Command Default

If this command is not configured, no default match certificate is configured for the PKI trustpool. Each of the **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords has a default behavior (see the "Syntax Description" section).

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

A certificate referenced in a **match certificate** command may not be deleted until all references to the certificate map are removed from configured trustpool (that is, no **match certificate** commands can reference the certificate map being deleted).

If the certificate map has no attributes defined, then the certificate is rejected.

Using the allow expired-certificate Keyword Combination

The **allow expired-certificate** keyword combination has three purposes:

- If the certificate of a peer has expired, this keyword may be used to allow the expired certificate until the peer is able to obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This keyword may be used to allow the certificate of the peer even though your router clock is not set.

Note If Network Time Protocol (NTP) is available only through the IPSec connection (usually through the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be "brought up" because the certificate of the hub is not yet valid.

- "Expired" is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end time specified in the certificate.

Using the skip revocation-check Keyword Combination

The type of enforcement provided using the **skip revocation-check** keyword combination is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. If one spoke communicates directly with another spoke, the CRLs must be checked. However, if the trustpoint is configured to require CRLs, the connection to the hub to retrieve the CRL usually cannot be made because the CRL is available only via the connection hub.

Using the skip authorization-check Keyword Combination

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **skip authorization-check** keyword combination. For example, if a VPN tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **skip authorization-check keyword** to skip the certificate check so that the tunnel can be established.

The **skip authorization-check** keyword combination should be configured after PKI integration with an AAA server is configured.

Examples

The following example shows how to configure revocation policy for an OSCP URL for an individual certificate authority (CA) certificate in the PKI trustpool by matching the issuer name:

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# match certificate mycert override ocsp 1 url http://ocspts.identrust.com
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.

Command	Description
default	Resets the value of a ca-trustpool configuration command to its default.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

match certificate (ISAKMP)

To assign an Internet Security Association Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate, use the **match certificate** command in crypto ISAKMP profile configuration mode. To remove the profile, use the **no** form of this command.

match certificate *certificate-map*

no match certificate *certificate-map*

Syntax Description

certificate-map	Name of the certificate map.

Command Default

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SX	This command is supported in the Cisco 12.2SX family of releases. Support in a 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **match certificate** command is used after the certificate map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer.

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   initiate mode aggressive
   match certificate cert_map
```

Related Commands

Command	Description
client configuration group	Associates a group with the peer that has been assigned an ISAKMP profile.

match certificate override cdp

To manually override the existing certificate distribution point (CDP) entries for a certificate with a URL or directory specification, use the **match certificate override cdp**command in ca-trustpoint configuration mode. To remove the override, use the **no** form of this command.

match certificate *certificate-map-label* **override cdp** {**url| directory**} *string*

no match certificate *certificate-map-label* **override cdp** {**url| directory**} *string*

Syntax Description

certificate-map-label	A user-specified label that must match the *label* argument specified in a previously defined **crypto ca certificate map** command.
url	Specifies that the certificates CDPs will be overridden with an http or ldap URL.
directory	Specifies that the certificate's CDPs will be overridden with an ldap directory specification.
string	The URL or directory specification.

Command Default

The existing CDP entries for the certificate are used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **match certificate override cdp**command to replace all of the existing CDPs in a certificate with a manually configured CDP URL or directory specification.

The *certificate-map-label* argument in the **match certificate override cdp**command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

Note Some applications may time out before all CDPs have been tried and will report an error message. This will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.

Examples

The following example uses the **match certificate override cdp**command to override the CDPs for the certificate map named Group1 defined in a **crypto ca certificate map** command:

```
crypto ca certificate map Group1 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group1 override cdp url http://server.cisco.com
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match certificate override ocsp

To override an Online Certificate Status Protocol (OCSP) server setting specified in either the Authority Info Access (AIA) field of the client certificate or in the trustpoint configuration , use the **match certificate override ocsp** command in ca-trustpoint configuration mode. To remove the OCSP server override setting, use the **no** form of this command.

match certificate *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*

no match certificate *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*

Syntax Description

certificate-map-label	Specifies the exact name of an existing certificate map label.
trustpoint *trustpoint-label*	(Optional) Specifies the existing trustpoint to be used when validating the OCSP server responder certificate.
sequence-number	Indicates the order of the override statements to be applied when a certificate is being verified. **Note** Certificate matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, the previous OCSP server override setting is replaced.
url *ocsp-url*	Specifies the OCSP server URL.

Command Default

No override OSCP server setting will be configured.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

OCSP server validation is usually based on the root certification authority (CA) certificate or a valid subordinate CA certificate, but may also be configured for validation of the OCSP server identity with the **match certificate override ocsp**command and **trustpoint** keyword.

One or more OCSP servers may be specified, either per client certificate or per group of client certificates. When the certificate matches a configured certificate map, the AIA field of the client certificate and any previously issued **ocsp url** command settings are overwritten with the specified OCSP server. If the **ocsp url** configuration exists and no map-based match occurs, the **ocsp url** configuration settings will continue to apply to the client certificates.

Examples

The following example shows an excerpt of the running configuration output when adding an override OCSP server to the beginning of an existing sequence:

```
match certificate map3 override ocsp 5 url http://192.168.2.3/
show running-config
.
.
.
        match certificate map3 override ocsp 5 url http://192.168.2.3/
        match certificate map1 override ocsp 10 url http://192.168.2.1/
        match certificate map2 override ocsp 15 url http://192.168.2.2/
The following example shows an excerpt of the running configuration output when an existing

override OSCP server
is replaced and a trustpoint is specified to use an alternative public key infrastructure
(PKI) hierarchy:
match certificate map4 override ocsp trustpoint tp4 10 url http://192.168.2.4/newvalue\
show running-config
.
.
.
        match certificate map3 override ocsp trustpoint tp3 5 url http://192.168.2.3/
        match certificate map1 override ocsp trustpoint tp1 10 url http://192.168.2.1/
       match certificate map4 override ocsp trustpoint tp4 10 url http://192.168.2.4/newvalue

        match certificate map2 override ocsp trustpoint tp2 15 url http://192.168.2.2/
The following example shows an excerpt of the running configuration output when an existing
 override OCSP server is removed from an existing sequence:
no match certificate map1 override ocsp trustpoint tp1 10 url http://192.168.2.1/
show running-config
.
.
.
        match certificate map3 override ocsp trustpoint tp3 5 url http://192.168.2.3/
       match certificate map4 override ocsp trustpoint tp4 10 url http://192.168.2.4/newvalue

        match certificate map2 override ocsp trustpoint tp2 15 url http://192.168.2.2/
```

Related Commands

Command	Description
crypto pki certificate map	Defines values in a certificate that should be matched or not matched.
ocsp url	Specifies the URL of an OCSP server so that the trustpoint can check the certificate status.

match certificate override sia

To manually override the existing SubjectInfoAccess (SIA) attribute, use the **match certificate override sia** command in CA-trustpoint configuration mode. To remove the override, use the **no** form of this command.

match certificate *certificate-map-label* **override sia** *sequence-number certificate-url*

no match certificate *certificate-map-label* **override sia**

Syntax Description

certificate-map-label	A user-specified label that should match the label argument specified in a previously defined **crypto ca certificate map** command.
sequence-number	The order of the override statements to be applied when a certificate is being verified. **Note** Certificate matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, the previous SIA override setting is replaced.
certificate-url	The remote location of the certificate in URL format.

Command Default

The existing SIA entries for the certificate are used.

Command Modes

CA-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The certificate's storage location is contained in the certificate itself by the issuing authority. This data is contained in the SIA and the AuthorityInfoAccess (AIA) extension in certificates. Use the **match certificate override sia** command to manually configure the remote location of the identity certificate regardless of the SIA attribute in the certificate.

Examples

The following example shows how to use the **match certificate override sia** command to override the SIAs for the certificate map named Group1 defined in a **crypto ca certificate map** command:

```
Router(config)# crypto ca certificate map Group1 10
```

```
Router(ca-certificate-map)# subject-name co ou=WAN
Router(ca-certificate-map)# subject-name co o=Cisco
!
Router(config)# crypto ca trustpoint pki
Router (ca-trustpoint)# match certificate Group1 override sia 100
http://certs.example.com/certificate.cer
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map or policy inline configuration mode. To remove a specific traffic class as a match criterion, use the **no** form of this command.

match class-map *class-map-nam e*

no match class-map *class-map-name*

Syntax Description

class-map-name	Name of the traffic class to use as a match criterion.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, do one of the following:

- Create a traffic class with the match-anyinstruction and use a class configured with the match-all instruction as a match criterion (using the **match class-map** command).

- Create a traffic class with the match-allinstruction and use a class configured with the match-any instruction as a match criterion (using the **match class-map** command).

You can also use the **match class-map** command to nest traffic classes within one another, saving users the overhead of re-creating a new traffic class when most of the information exists in a previously configured traffic class.

When packets are matched to a class map, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Examples

Examples

In the following example, the traffic class called class1 has the same characteristics as traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, you can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and you can simply add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result of traffic class called class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class called class 4: IP protocol *and* QoS group 4, destination MAC address 1.1.1, or access group 2. Match criteria IP protocol *and* QoS group 4 are required in the definition of the traffic class named class3 and included as a possible match in the definition of the traffic class named class4 with the **match class-map class3** command.

In this example, only the traffic class called class4 is used with the service policy called policy1.

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match class session

Note Effective with Cisco IOS Release 15.2(4)M, the **match class session** command is not available in Cisco IOS software.

To configure match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session, use the **match class session** command in class map configuration mode. To remove this configuration, use the **no** form of this command.

match class *class-name* [**packet-range** *low high*| **byte-range** *low high*] **session**

no match class *class-name* [**packet-range** *low high*| **byte-range** *low high*] **session**

Syntax Description

class-name	Specifies the class map used to identify a session containing packets of interest. The classification results are preserved for the subsequent packets of the same packet session.
packet-range *low high*	(Optional) Specifies the range of packets from 1 to 2147483647, in which the regular expressions (regex) within every packet is are checked. The classification results are preserved for the specified packets or bytes of the same packet session.
byte-range *low high*	(Optional) Specifies the range of bytes from 1 to 2147483647, in which the regular expressions (regex) within every packet are checked. The classification results are preserved for the specified packets or bytes of the same packet session.

Command Default

The regex matching is within a single packet with a range 1 to infinity.

Command Modes

Class map configuration (config-cmap)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

With the introduction of Cisco IOS Release15.1(3)T, Flexible Packet Matching (FPM) can now match every packet against the filters specified in the class map and pass the match result to consecutive packets of the same network session. If a filter matches with malicious content in the packet's protocol header or payload, then the required action is taken to resolve the problem.

The **match class session** command configures match criteria that identify a session containing packets of interest, which is then applied to all packets transmitted during the session. The **packet-range** and **byte-range** keywords are used to create a filter mechanism that increases the performance and matching accuracy of regex-based FPM class maps by classifying traffic that resides in the narrow packet number or byte ranges of each packet flow. If packets go beyond the classification window, then the packet flow can be identified as unknown and packet classification is terminated early to increase performance. For example, a specific application can be blocked efficiently by filtering all packets that belong to this application on a session. These packets are dropped without matching every individual packet with the filters, which improves the performance of a session.

These filters also reduce the number of false positives introduced by general regex-based approaches. For example, Internet company messenger traffic can be classified with a string like **intco**, **intcomsg**, and **ic**. These strings are searched for in a packet's payload. These small strings can appear in the packet payload of any other applications, such as e-mail, and can introduce false positives. False positives can be avoided by specifying which regex is searched within which packet of a particular packet flow.

Once the match criteria are applied to packets belonging to the specific traffic class, these packets can be discarded by configuring the **drop all** command in a policy map. Packets match only on the packet flow entry of an FPM, and skip user-configured classification filters.

A match class does not have to be applied exclusively for a regex-based filter. Any FPM filter can be used in the nested match class filter. For example, if the match class **c1** has the filter **match field TCP source-port eq 80**, then the **match class c1 session** command takes the same action for the packets that follow the first matching packet.

Examples

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **drop all** command is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"
Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# drop all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. However, this example uses the **match class** command with the **packet-range** keyword, which acts as a filter mechanism to increases the performance and matching accuracy of the regex-based FPM class map.

```
Router(config)# load disk2:ip.phdf
```

```
Router(config)# load protocol disk2:tcp.phdf
Router(config)# class-map type stack match-all ip_tcp
Router(config-cmap)# description "match TCP over IP packets"
Router(config-cmap)# match field ip protocol eq 6 next tcp
Router(config)# class-map type access-control match-all WM
Router(config-cmap) # match start tcp payload-start offset 20 size 20 regex
".*(WEBCO|WMSG|WPNS).......[LWT].*\xc0\x80"
Router(config)# class-map type access-control match-all wtube
Router(config-cmap) # match start tcp payload-start offset 20 size 20 regex
".*GET\x20.*HTTP\x2f(0\.9|1\.0|1\.1)\x0d\x0aHost:\x20webtube.com\x0d\x0a"
Router(config)# class-map type access-control match-all doom
Router(config-cmap) # match start tcp payload-start offset 20 size 20 string virus
Router(config)# class-map type access-control match-all class_webco
Router(config-cmap)# match class WM session
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start network-start offset 224 size 4 eq 0x4011010
Router(config)# class-map type access-control match-all class_webtube
Router(config-cmap)# match class wtube packet-range 1 5 session
Router(config-cmap)# match class doom session
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start network-start offset 224 size 4 eq 0x4011010
Router(config)# policy-map type access-control my_policy
Router(config-pmap)# class class_webco
Router(config-pmap-c)# log
Router(config)# policy-map type access-control my_policy
Router(config-pmap)# class class_webtube
Router(config-pmap-c)# drop all
Router(config)# policy-map type access-control P1
Router(config-pmap)# class ip_tcp
Router(config-pmap-c)# service-policy my_policy
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input P1
```

Related Commands

Command	Description
drop	Configures a traffic class to discard packets belonging to a specific class.
log	Generates log messages for the traffic class.

match cmd

To specify a value that limits the length of the ESMTP command line or specifies the ESMTP command line verb used to thwart denial of service (DoS) attacks, use the **match cmd**command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match cmd {**line length gt** *length*| **verb** {**AUTH**| **DATA**| **EHLO**| **ETRN**| **EXPN**| **HELO**| **HELP**| **MAIL NOOP**| **QUIT**| **RCPT**| **RSET**| **SAML**| **SEND**| **SOML**| **STARTTLS**| **VERB**| **VRFY**| **WORD**}}

no match cmd {**line length gt** *length*| **verb** {**AUTH**| **DATA**| **EHLO**| **ETRN**| **EXPN**| **HELO**| **HELP**| **MAIL NOOP**| **QUIT**| **RCPT**| **RSET**| **SAML**| **SEND**| **SOML**| **STARTTLS**| **VERB**| **VRFY**| **WORD**}}

Syntax Description

line length gt *length*	Specifies the ESMTP command line greater than the length of a number of characters from 1 to 65535.
verb	Specifies the ESMTP command verb used to thwart DoS attacks.
AUTH	SMTP service extension whereby an SMTP client may indicate an authentication mechanism to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions.
DATA	Sent by a client to initiate the transfer of message content.
EHLO	Enables the server to identify its support for Extended Simple Mail Transfer Protocol (ESMTP) commands.
ETRN	Requests the local SMTP server to initiate delivery of mail to the external SMTP server on a separate SMTP connection.
EXPN	Expand a mailing list address into individual recipients. Often disabled to prevent use by spammers.
HELO	Sent by a client to identify itself, usually with a domain name.
HELP	Returns a list of commands that are supported by the SMTP service.

MAIL NOOP	Start of MAIL FROM: Identifies sender of mail message. May be forged. May not correspond to the From: line in a mail message. Should be added in Return Path header. Address to send any undeliverable notifications (bounces). The NO OPeration (NOOP) does nothing, except keep the connection active and help synchronize commands and responses.
QUIT	Terminates the session.
RCPT	Identifies the message recipients; used in the form RCPT TO:
RSET	Nullifies the entire message transaction and resets the buffer.
SAML	Start of SAML FROM: Like MAIL except supposed to also display the message on the recipients computer (early form of instant messaging).
SOML	Start of SAML FROM: Like MAIL except supposed to either mail the message OR display the message on the recipients computer (early form of instant messaging)
STARTTLS	Triggers start of TLS negotiation for secure SMTP conversation. If successful, resets state to before EHLO command sent.
VERB	Enables verbose (detailed) responses.
VRFY	Verifies that a mailbox is available for message delivery; for example, the **VRFY MARK** command verifies that a mailbox for MARK resides on the local server. This command is off by default in Exchange implementations.
WORD	Specifies a word in the body of the e-mail message.

Command Default The length of the ESMTP command line or command line verb is not defined.

Command Modes Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

In a **class-map type inspect smtp match-all** command statement with the **match cmd verb** command statement, only the following **match cmd line length gt** command statement can coexist. For example:

```
class-map type inspect smtp match-all c2
  match cmd line length gt 256
  match cmd verb MAIL
```

Note There are no match restrictions in case of a **class-map type inspect smtp match-any** command statement for a class map because the class-map applies to all SMTP commands.

The class-map **c2** matches if the length of only the e-mail command is greater than 256 bytes (which is not applicable to other commands), which translates to: If the length of the MAIL command exceeds the configured value.

Note If no **match cmd verb** command statement is specified in a **class-map type inspect smtp match-all** command statement for a class-map, which contains the **match cmd line length gt** command statement, then the class-map applies to all SMTP commands.

Examples

The following example shows how to configure an SMTP application firewall policy to limit the length of an SMTP command line to prevent a Denial of Service (DoS) attack:

```
class-map type inspect smtp c1
 match header length gt 16000
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.

match data-length

To determine if the amount of data transferred in a Simple Mail Transfer Protocol (SMTP) connection is greater than the configured limit, use the **match data-length**command in class-map type inspect smtp configuration mode. To remove this match criteria, use the **no** form of this command.

match data-length gt *max-data-value*

no match data-length gt *max-data-value*

Syntax Description

gt *max-data-value*	Maximum number of bytes (data) that can be transferred in a single SMTP session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. The default is 20.

Command Default

The inspection rule is not defined.

Command Modes

Class-map type inspect smtp configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **match data-length** match criteria can be specified only under an SMTP class map. For more information, see the **class-map type inspect smtp** command.

Examples

The following example specifies that a maximum of 200000 bytes can be transferred in a single SMTP session:

```
class-map type inspect smtp c11
 match data-length gt 200000
policy-map type inspect smtp p11
 class type inspect smtp c11
  reset
```

Related Commands

Command	Description
class-map type inspect smtp	Configures inspection parameters for SMTP.
ip inspect name	Defines a set of inspection rules.

match eku

To allow a public key infrastructure (PKI) client to validate a peer certificate only if the specified extended key usage (EKU) attribute is present in the certificate, use the **match eku** command in certification authority (CA) trustpoint configuration mode. To disable the configuration, use the **no** form of this command.

match eku *attribute*

no match eku *attribute*

Syntax Description

attribute	The *attribute* argument can be one of the following: • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • ssh-client • ssh-server • time-stamping

Command Default

EKU attributes are not required to successfully validate the certificate.

Command Modes

Certification authority trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
Cisco IOS 15.2(2)T	This command was introduced.

Usage Guidelines

Use the **crypto pki trustpoint** command in global configuration mode to declare the trustpoint and a given name and to enter CA-trustpoint configuration mode.

The **match eku** command under the PKI trust point enforces the presence of the EKU field in validating a certificate.

Examples

The following example shows how to configure the PKI to validate a peer certificate using the EKU attribute “ssh-client” in the certificate:

```
Device> enable
Device# configure terminal
Device(config)# crypto pki trustpoint msca
Device(ca-trustpoint)# eku request ssh-client
Device(ca-trustpoint)# match eku ssh-client
Device(ca-trustpoint)# end
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint and a given name.
eku request	Configures the request to include a specific EKU attribute in the certificate.

match encrypted

Note Effective with Cisco IOS Release 15.2(4)M, the **match encrypted** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of encrypted Flexible Packet Matching (FPM) filters and enter FPM match encryption filter configuration mode, use the **match encrypted** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match encrypted

no match encrypted

Syntax Description

This command has no arguments or keywords.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Examples

The following example shows how to enter FPM match encryption filter configuration mode:

```
Router(config)# class-map type access-control match-all class2
Routre(config-cmap)# match encrypted
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
algorithm	Specifies the algorithm to be used for decrypting the filters.
cipherkey	Specifies the symmetric keyname that is used to decrypt the filter.
ciphervalue	Specifies the encrypted filter contents.
class-map type	Creates a class map to be used for matching packets to a specified class.
filter-hash	Specifies the hash for verification and validation of decrypted contents.
filter-id	Specifies a filter level ID for encrypted filters.
filter-version	Specifies the filter level version value for encrypted filters.

match field

Note Effective with Cisco IOS Release 15.2(4)M, the **match field** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs), use the **match field** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match field *protocol protocol-field* {**eq [mask]**| **neq [mask]**| **gt**| **lt**| **range** *range*| **regex** *string*} *value* [**next** *next-protocol*]

no match field *protocol protocol-field* {**eq [mask]**| **neq [mask]**| **gt**| **lt**| **range** *range*| **regex** *string*} *value* [**next** *next-protocol*]

Syntax Description

protocol	Name of protocol whose PHDF has been loaded onto a router.
protocol field	*Match criteria is based upon the specified f*ield *within the loaded protocol.*
eq	*Match criteria is met if the* packet is equal to the specified value or mask.
neq	*Match criteria is met if the* packet is not equal to the specified value or mask.
mask *mask*	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	*Match criteria is met if the* packet does not exceed the specified value.
lt	*Match criteria is met if the* packet is less than the specified value.
range *range*	Match criteria is based upon a lower and upper boundary protocol field range.
regex *string*	Match criteria is based upon a string that is to be matched.
value	Value for which the packet must be in accordance with.

next *next-protocol*	Specify the next protocol within the stack of protocols that is to be used as the match criteria.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
Cisco IOS XE 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

Before issuing the **match-field** command, you must load a PHDF onto the router via the **load protocol** command. Thereafter, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Match criteria are defined via a start point, offset, size, value to match, and mask. A match can be defined on a pattern with any protocol field.

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
```

```
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match start	Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).

match file-transfer

To use file transfers as the match criterion, use the **match file-transfer**command in class-map configuration mode. To remove the file transfer match criterion from the configuration file, use the **no** form of this command.

match file-transfer [*regular-expression*]

no match file-transfer [*regular-expression*]

Syntax Description

regular-expression	(Optional) The regular expression used to identify file transfers for a specified P2P application. For example, entering ".exe" as the regular expression would classify the Gnutella file transfer connections containing the string ".exe" as matches for the traffic policy. To specify that all file transfer connections be identified by the traffic class, use an asterisk (*) as the regular expression.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

After the **class-map type inspect**command is issued and a P2P application is specified, you can use the **match file-transfer**command to configure the Cisco IOS Firewall to match file transfer connections within any supported P2P protocol.

Note This command can be used only with the following supported P2P protocols: eDonkey, Gnutella, Kazaa Version 2, and FastTrack.

Examples

The following example shows how to configure the Cisco IOS Firewall to block and reset all Gnutella file transfers that are classified into the "my-gnutella-restrictions" class map:

```
class-map type inspect gnutella match-any my-gnutella-restrictions
```

```
 match file-transfer *
!
policy-map type inspect p2p my-p2p-policy
 reset
 log
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match group-object security

To match traffic from a user in the source and destination security group, use the **match group-object security** command in class-map configuration mode. To remove the match criteria for the source or destination security group, use the **no** form of this command.

match group-object security {**source** *name*| **destination** *name*}

no match group-object security {**source** *name*| **destination** *name*}

Syntax Description

source	Specifies the source security group.
destination	Specifies the destination security group.
name	Name of the source or destination group.

Command Default

No source or destination security group is defined.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was introduced in Cisco IOS XE Release 3.5.

Usage Guidelines

The **match group-object security** command is used in the class map configuration of the Security Group Access (SGA) Zone-Based Policy firewall (ZBPF).

Note A policy map must also be configured for the SGA ZBPF.

Examples

The following example shows how the **match group-object security** command is used in the class map configuration of the SGA ZBPF.

```
Router(config)# object-group security myobject1
Router(config-object-group)# security-group tag-id 1
Router(config-object-group)# end
Router(config)# class-map type inspect match-any myclass1
Router(config-cmap)# match group-object security source myobject1
Router(config-cmap)# end
```

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
group-object	Specifies a nested reference to a type of user group.
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
security-group	Specifies the membership of the security group for an object group.
show object-group	Displays the content of all user groups.

match header count

To configure an HTTP firewall policy to permit or deny HTTP traffic on the basis of request, response, or both request and response messages whose headers do not exceed a maximum number of fields, use the **match header count** command in class-map configuration mode. To change the configuration, use the **no** form of this command.

match {**request**| **response**| **req-resp**} **header** [*header-name*] **count gt** *number*

no match {**request**| **response**| **req-resp**} **header** [*header-name*] **count gt** *number*

Syntax Description

request	Headers in request messages are checked for the match criterion.
response	Headers in response messages are checked for the match criterion.
req-resp	Headers in both request and response messages are checked for the match criterion.
header-name	(Optional) Specific line in the header field. This argument enables the firewall to scan for repeated header fields. **Note** If this option is defined, the **gt** *number* option must be set to 1.
gt *number*	Message cannot be greater than the specified number of header lines (fields).

Command Default

HTTP header-lines are not considered when permitting or denying HTTP traffic.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **match header count**command to configure an HTTP firewall policy match criterion on the basis of a maximum allowed header fields count.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Header Field Repetition Inspection

To enable the firewall policy to checks whether a request or response message has repeated header fields, use the *header-name*argument. This functionality can be used to prevent session smuggling.

Examples

The following example shows how to configure an HTTP application firewall policy to block all requests that exceed 16 header fields:

```
class-map type inspect http hdr_cnt_cm
 match req-resp header count gt 16
policy-map type inspect http hdr_cnt_pm
 class type inspect http hdr_cnt_cm
 reset
```

The following example shows how to configure an HTTP application firewall policy to block a request or response that has multiple content-length header lines:

```
class-map type inspect http multi_occrns_cm
 match req-resp header content-length count gt 1
policy-map type inspect http multi_occrns_pm
 class type inspect http multi_occrns_cm
 reset
```

match header length gt

To thwart DoS attacks, use the **match header length gt**command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match header length gt *bytes*

no match length gt *bytes*

Syntax Description

bytes	Specifies a value from 1 to 65535 that limits the maximum length of the SMTP header in bytes.

Command Default

Header length is not considered when permitting or denying SMTP messages.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The *header-name* argument and the **req-resp** keyword were added.
12.4(20)T	The **request**, **response**, and **req-resp** keywords were removed and the *header-name* argument was removed. This command now applies to SMTP only.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **match header length** commandmatches on the maximum length of an SMTP header. If that number is exceeded, the match succeeds.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an SMTP application firewall policy to block all SMTP headers that exceed a length of 4096 bytes:

```
class-map type inspect smtp c1
 match header length gt 4096
policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

Related Commands

Command	Description
max-header-regex	Specifies an arbitrary text expression in the SMTP e-mail message header (subject field) or e-mail body such as ‘subject’, ‘Received’, ‘To’ or other private header fields to monitor text patterns.

match header regex

To specify an arbitrary text expression (regular expression) in message or content type headers to monitor text patterns, use the **match header regex**command in class map configuration mode. To remove this filter from the configuration, use the **no** form of this command.

Note The **request**, **response**, and **req-resp** keywords and *header-name* argument are not used in the configuration of an SMTP class map.

match {**request**| **response**| **req-resp**} **header [header-name] regex parameter-map-name**

no match {**request**| **response**| **req-resp**} **header [header-name] regex parameter-map-name**

Syntax Description

request	Headers in request messages are checked for the match criterion.
response	Headers in response messages are checked for the match criterion.
req-resp	Headers in both request and response messages are checked for the match criterion.
header-name	Specific line or content type in the header field. This argument enables the firewall to scan for repeated header fields.
parameter-map-name	Name of a specific traffic pattern specified through the **parameter-map type regex**command.

Command Default

Policies do not monitor content type headers.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	The **request**, **response**, and **req-resp** keywords and *header-name* argument were removed for the configuration of an SMTP class map.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

Configuring a Class Map for SMTP

Use the **match header regex**command to configure an SMTP policy match criterion on the basis of headers that match the regular expression defined in a parameter map. An arbitrary text expression in the SMTP e-mail message header (subject field) or e-mail body such as 'subject', 'Received', 'To' or other private header fields helps the router to monitor text patterns.

Configuring a Class Map for HTTP

An HTTP firewall policy match criteria can be configured on the basis of headers that match the regular expression defined in a parameter map.

HTTP has two regular expression (regex) options. One combines the **header** keyword, **content type** header name, and **regex** keyword and *parameter-map-name* argument. The other combines the **header** keyword and **regex** keyword and *parameter-map-name* argument.

- If the **header** and **regex** keywords are used with the *parameter-map-name* argument, it does not require a period and asterisk infront of the *parameter-map-name* argument. For example, either "html" or ".*html" *parameter-map-name argument* can be configured.
- If the **header** keyword is used with the **content-type** header name and **regex** keyword, then the parameter map name requires a period and asterisk (.*) in front of the *parameter-map-name* argument. For example, the *parameter-map-name* argument "html" is expressed as: .*html

Note If the period and asterisk is added in front of html (.*html), the *parameter-map-name* argument works for both HTTP regex options.

- The **mismatch** keyword is only valid for the **match response header content-type regex** command syntax for messages that need to be matched that have a **content-type**header name mismatch.

Tip It is a good practice to add ".*" to the **regex***parameter-map-name* arguments that are not present at the beginning of a text string.

Examples

SMTP Class Map Example

The following example shows how to configure an SMTP policy using the **match header regex** command:

```
parameter-map type regex lottery-spam
 pattern "Subject:*lottery*"
class-map type inspect smtp c1
 match header regex lottery-spam
policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
HTTP Class Map Example
```

The following example shows how to configure an HTTP policy using the **match header regex** command:

```
parameter-map type inspect .*html
```

```
class-map type inspect http http-class
 match req-resp header regex .*html
policy-map type inspect http myhttp-policy
 class-type inspect http http-class
 reset
```

Related Commands

Command	Description
max-header-regex	Specifies an arbitrary text expression in the SMTP e-mail message header (subject field) or e-mail body such as ‘subject’, ‘Received’, ‘To’ or other private header fields to monitor text patterns.
parameter-map type	Creates or modifies a parameter map.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect type policy map.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity**command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

match identity {**group** *group-name*| **address** {*address* [*mask*] [*fvrf*]| **ipv6** *ipv6-address*}| **host** *host-name*| **host domain** *domain-name*| **user** *user-fqdn*| **user domain** *domain-name*}

no match identity {**group** *group-name*| **address** {*address* [*mask*] [*fvrf*]| **ipv6** *ipv6-address*}| **host** *host-name*| **host domain** *domain-name*| **user** *user-fqdn*| **user domain** *domain-name*}

Syntax Description

group *group-name*	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the *group-name* argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address *address* [*mask*] [*fvrf*]	Identity that matches the identity of type ID_IPV4_ADDR. • *mask*-- Use to match the range of the address. • *fvrf* --Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
ipv6 *ipv6-address*	Identity that matches the identity of type ID_IPV6_ADDR.
host *host-name*	Identity that matches an identity of the type ID_FQDN.
host domain *domain-name*	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user *user-fqdn*	Identity that matches the FQDN.
user domain *domain-name*	Identity that matches the identities of the type ID_USER_FQDN. When the **user domain** keyword is present, all users having identities of the type ID_USER_FQDN and ending with "*domain-name*" will be matched.

Command Default

No default behavior or values

Command Modes ISAKMP profile configuration (conf-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and *ipv6-address a*rgument were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines There must be at least one **match identity**command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples The following example shows that the **match identity**command is configured:

```
crypto isakmp profile vpnprofile
 match identity group vpngroup
 match identity address 10.53.11.1
 match identity host domain example.com
 match identity host server.example.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

match (IKEv2 policy)

To match a policy based on Front-door VPN Routing and Forwarding (FVRF) or local parameters, such as an IP address, use the **match** command in IKEv2 policy configuration mode. To delete a match, use the **no** form of this command.

match address local {*ipv4-address*| *ipv6-address*| **fvrf** *fvrf-name*| **any**}

no match address local {*ipv4-address*| *ipv6-address*| **fvrf** *fvrf-name*| **any**}

Syntax Description

address local	Matches a policy based on the local IPv4 or IPv6 address.
ipv4-address	IPv4 address.
ipv6-address	IPv6 address.
fvrf	Matches a policy based on the user-defined FVRF.
frvf-name	FVRF name
any	Matches a policy based on any FVRF.

Command Default

If no match address is specified, the policy matches all local addresses.

Command Modes

IKEv2 policy configuration (crypto-ikev2-policy)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to match a policy based on the FVRF or the local IP address (IPv4 or IPv6). The FVRF specifies the VRF in which the IKEv2 security association (SA) packets are negotiated. The default FVRF is the global FVRF. Use the **match fvrf any** command to match a policy based on any FVRF.

A policy with no match address local statement will match all local addresses. A policy with no match FVRF statement will match the global FVRF. If there are no match statements, an IKEv2 policy matches all local addresses in the global VRF.

Examples

The following example shows how to match an IKEv2 policy based on the FVRF and the local IPv4 address:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
Router(config-ikev2-policy)# match fvrf fvrf1
Router(config-ikev2-policy)# match address local 10.0.0.1
```

The following example shows how to match an IKEv2 policy based on the FVRF and the local IPv6 address:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
Router(config-ikev2-policy)# match fvrf fvrf1
Router(config-ikev2-policy)# match address local 2001:DB8:0:ABCD::1
```

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
proposal	Specifies the proposals that must be used in the IKEv2 policy.
show crypto ikev2 policy	Displays the default or user-defined IKEv2 policy.

match (IKEv2 profile)

To match a profile on front-door VPN routing and forwarding (FVRF) or local parameters such as the IP address, the peer identity, or the peer certificate, use the **match** command in IKEv2 profile configuration mode. To delete a match, use the **no** form of this command.

match {**address local** {*ipv4-address*| *ipv6-address*| **interface** *name*}| **certificate** *certificate-map*| **fvrf** {*fvrf-name*| **any**}| **identity remote address** {*ipv4-address* [*mask*]| *ipv6-address-prefix*}| **email** [*domain*] *string*| **fqdn** [*domain*] *string*| **key-id** *opaque-string*| **any**}

no match {**address local** {*ipv4-address*| *ipv6-address*| **interface** *name*}| **certificate** *certificate-map*| **fvrf** {*fvrf-name*| **any**}| **identity remote address** {*ipv4-address* [*mask*]| *ipv6-address-prefix*}| **email** [*domain*] *string*| **fqdn** [*domain*] *string*| **key-id** *opaque-string*| **any**}

Syntax Description

address local {*ipv4-address* | *ipv6-address*}	Matches the profile based on the local IPv4 or IPv6 address.
interface *name*	Matches the profile based on the local interface.
certificate *certificate-map*	Matches the profile based on fields in the certificate received from the peer.
fvrf *fvrf-name*	Matches the profile based on the user-defined FVRF. The default FVRF is global.
any	Matches the profile based on any FVRF. **Note** The **match vrf any** command must be explicitly configured to match all VRFs.
identity remote	Match a profile based on the remote IKEv2 identity field in the AUTH exchange.
address {*ipv4-address* [*mask*] | *ipv6-address prefix*}	Matches a profile based on the identity of the type remote IPv4 address and its subnet mask or IPv6 address and its prefix length.
key-id *opaque-string*	Matches a profile based on the identity of the type remote key ID.
email	Matches a profile based on the identity of the type remote email ID.
fqdn *fqdn-name*	Matches a profile based on the identity of the type remote Fully Qualified Domain Name (FQDN).
domain *string*	Matches a profile based on the domain part of remote identities of the type FQDN or email.
any	Matches the profile based on any remote address.

Command Default A match is not specified.

Command Modes IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.3(3)M	This command was modified. The **any** keyword was added for remote address.

Usage Guidelines In an IKEv2 profile, multiple match statements of the same type are logically ORed and match statements of different types are logically ANDed.

Note The **match identity remote** and **match certificate** statements are considered the same type of statements and are ORed.

The result of configuring multiple **match certificate** statements is the same as configuring one **match certificate** statement. Hence, using a single **match certificate** statement as a certificate map caters to multiple certificates and is independent of trustpoints.

Note There can only be one match FVRF statement.

For example, the following command translates to the subsequent “and”, “or” statement:

```
crypto ikev2 profile profile-1
 match vrf green
 match local address 10.0.0.1
 match local address 10.0.0.2
 match certificate remote CertMap
```

(vrf = green AND (local addr = 10.0.0.1 OR local addr = 10.0.0.1) AND remote certificate match CertMap).

There is no precedence between match statements of different types, and selection is based on the first match. Configuration of overlapping profiles is considered as a misconfiguration.

Examples

The following examples show how an IKEv2 profile is matched on the remote identity. The following profile caters to peers that identify using **fqdn example.com** and authenticate with **rsa-signature** using **trustpoint-remote**. The local node authenticates with **pre-share** using **keyring-1**.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
identity (IKEv2 profile)	Specifies how the local or remote router identifies itself to the peer and communicates with the peer in the RSA authentication exchange.
authentication (IKEv2 profile)	Specifies the local and remote authentication methods in an IKEv2 profile.
keyring (IKEv2 profile)	Specifies a locally defined or AAA-based keyring.
pki trustpoint	Specifies the router to use the PKI trustpoints in the RSA signature authentication.

match invalid-command

To locate invalid commands on a Post Office Protocol, Version 3 (POP 3) server or an Internet Message Access Protocol (IMAP) connection, use the **match invalid-command** in class-map configuration mode. To stop locating invalid commands, use the **no** form of this command.

match invalid-command

no match invalid-command

Syntax Description

This command has no arguments or keywords.

Command Default

It is not required that invalid commands be located.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **class-map type inspect imap** or **class-map type inspect pop3** command.

Examples

The following example causes the Zone-Based Policy Firewall software to locate invalid commands on the POP3 server:

```
class-map type inspect pop3 pop3-class
 match invalid-command
```

Related Commands

Command	Description
class-map type inspect imap	Configures inspection parameters for IMAP.
class-map type inspect pop3	Configures inspection parameters for POP3.

match ipv6 access-list

To verify the sender's IPv6 address in inspected messages from the authorized prefix list, use the **match ipv6 access-list** command in RA guard policy configuration mode.

match ipv6 access-list *ipv6-access-list-name*

Syntax Description

ipv6-access-list-name	The IPv6 access list to be matched.

Command Default

Senders' IPv6 addresses are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **match ipv6 access-list** command enables verification of the sender's IPv6 address in inspected messages from the configured authorized router source access list. If the **match ipv6 access-list** command is not configured, this authorization is bypassed.

An access list is configured using the **ipv6 access-list** command. For instance, to authorize the router with link-local address FE80::A8BB:CCFF:FE01:F700 only, define the following IPv6 access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any
```

Note The access list is used here as a convenient way to define several explicit router sources, but it should not be considered to be a port-based access list (PACL). The **match ipv6 access-list** command verifies the IPv6 source address of the router messages, so specifying a destination in the access list is meaningless and the destination of the access control list (ACL) entry should always be "any." If a destination is specified in the access list, then matching will fail.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and matches the IPv6 addresses in the access list named list1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ipv6 access-list list1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.

match login clear-text

To find a nonsecure login when using an Internet Message Access Protocol (IMAP) or Post Office Protocol, Version 3 (POP3) server, use the **match login clear-text** command in class-map configuration mode. To disable this match criteria, use the **no** form of this command.

match login clear-text

no match login clear-text

Syntax Description

This command has no arguments or keywords.

Command Default

Finding non-secure logins is not required.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command either when you are configuring a POP3 firewall class map after you enter the **class-map type inspect pop3** command or when you are configuring an IMAP firewall class map after you enter the **class-map type inspect imap** command.

Examples

The following example determines if the login process is happening in clear-text:

```
class-map type inspect pop3 pop3-class
 match login clear-text
```

Related Commands

Command	Description
class-map type inspect imap	Configures inspection parameters for IMAP.
class-map type inspect pop3	Configures inspection parameters for POP3.
ip inspect name	Defines a set of inspection rules.

match message

To configure the match criterion for a class map on the basis of H.323 protocol messages, use the match message command in class-map configuration mode. To remove the H.323-based match criterion from a class map, use the no form of this command.

match message *message-name*

no match message *message-name*

Syntax Description

message-name	Name of the message used as a message criterion. The supported message criteria are as follows: • **alerting** --H.225 ALERTING message • call-proceeding --H.225 CALL PROCEEDING message • connect --H.225 CONNECT message • facility --H.225 FACILITY message • release-complete --H.225 RELEASE COMPLETE message • **setup** --H.225 SETUP message • status --H.225 STATUS message • status-enquiry --H.225 STATUS ENQUIRY message

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the match message command to inspect H.323 traffic based on the message criterion.

The match message command is available under the class-map type inspect h323 command.

Examples

The following example shows how to configure an H.323 specific class-map to match H.225 SETUP or H.225 RELEASE COMPLETE messages only.

```
class-map type inspect h323 match-any my_h323_rt_msgs
match message setup
match message release-complete
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match mime content-type regex

To specify Multipurpose Internet Mail Extension (MIME) content file types, which are restricted in attachments in the body of the e-mail being sent over SMTP, use the **match mime content-type regex** commandin class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match mime content-type regex *content-type-regex*

no match mime content-type regex *content-type-regex*

Syntax Description

content-type-regex	Specifies the type of content in the MIME header in regular expression form.

Command Default

The content type regular expression is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The format of data being transmitted through SMTP is specified by using the MIME standard, which uses headers to specify the content-type, encoding and the filenames of data being sent (text, html, images, applications, documents etc.). The following is an example of an e-mail using the MIME format:

```
From: "foo" <foo@cisco.com>
To: bar <bar@abc.com>
Subject: testmail
Date: Sat, 7 Jan 2006 20:18:47 -0400
Message-ID: <000dadf7453e$bee1bb00$8a22f340@oemcomputer>
MIME-Version: 1.0
Content-Type: image/jpeg;
name='picture.jpg'
Content-Transfer-Encoding: base64
```
<base64 encoded data for the picture.jpg image>

In the above example, the “name=’picture.jpg’” is optional. Even without the definition, the image is sent to the recipient. The e-mail client of the recipient may display it as “part-1”, “attach-1” or it may render the image in-line. Also, attachments are not ‘stripped’ from the e-mail. If a content-type for which ‘reset’ action was configured is detected, an 5XX error code is sent and the connection is closed, in order to prevent the whole e-mail from being delivered. However, the remainder of the e-mail message is sent.

Examples

The following example shows how to configure an SMTP application firewall policy to specify that any form of JPEG image content be restricted in attachments in the body of the e-mail being sent over SMTP:

```
parameter-map type regex jpeg
 pattern “*image//*”
class-map type inspect smtp c1
 match mime content-type regex
 jpeg
policy-map type inspect smtp p1
 class type inspect smtp c1
 log
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
parameter-map type regex	Enters the parameter-map name of a specific traffic pattern.
pattern	Cisco IOS regular expression (regex) pattern that matches the traffic pattern for the e-mail sender or user accounts from suspected domains that are causing the spam e-mail.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match mime encoding

To restrict unknown Multipurpose Internet Mail Extension (MIME) content-encoding types or values from being transmitted over SMTP, use the **match mime encoding**commandin class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match mime encoding {**unknown**| *WORD*| *encoding-type*}

nomatch mime encoding {**unknown**| *WORD*| *encoding-type*}

Syntax Description

unknown	Specify this keyword if the content-transfer-encoding value in the e-mail does not match any of the ones in the list to restrict unknown and potentially dangerous encodings.
WORD	Specifies a user-defined content-transfer encoding type, which must begin with 'X' (example, "Xmyencodingscheme"). Non-alphanumeric characters, such as hyphens, are not supported.

encoding-type	Specifies one of the pre-configured content-transfer-encoding type: • • **7-bit** -ASCII characters • **8-bit** -Facilitates the exchange of e-mail messages containing octets outside the 7-bit ASCII range. • **base64** -Any similar encoding scheme that encodes binary data by treating it numerically and translating it into a base 64 representation. • **quoted-printable** -Encoding using printable characters (i.e. alphanumeric and the equals sign "=") to transmit 8-bit data over a 7-bit data path. It is defined as a MIME content transfer encoding for use in Internet e-mail. • **binary** -Representation for numbers using only two digits (usually, 0 and 1). • **x-uuencode** -Nonstandard encoding. • The **quoted-printable** and **base64** encoding types tell the email client that a binary-to-text encoding scheme was used and that appropriate initial decoding is necessary before the message can be read with its original encoding.

Command Default

The MIME encoding type or value is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The pre-configured content-transfer-encoding types act as a filter on the ‘content-transfer-encoding’ field in the MIME header within the SMTP body. The ‘uuencode’ encoding type is not recognized as a standard type by the MIME RFCs because many subtle differences exist in its various implementations. However, since it is used by some mail systems, the **x-uuencode** type is included in the pre-configured list.

Examples

The following example shows how to configure an SMTP application firewall policy to specify that any quoted-printable encoding field in the MIME header within the SMTP body be restricted in e-mail being sent over SMTP:

```
class-map type inspect smtp c1
 match mime encoding quoted-printable
policy-map type inspect smtp p1
 class type inspect smtp c1
 log
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
log	Generates a log of messages.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match not

To negate the classification criteria for an inspect-type class map that is configured for the General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **match not** command in QoS class-map configuration mode. To enable the classification criteria, use the **no** form of this command.

match not {**apn regex** *regex-parameter-map*| **mcc** *country-code* **mnc** *network-code*| **message-id** *id*| **message-length min** *min-length* **max** *max-length*| **version** *number*}

message-length min no match not {**apn** | **mcc** *country-code* **mnc** *network-code*| **message-id** *id*| **message-length**| **version** *number*}

Syntax Description

apn	Prevents the filtering of the GTP Access Point Name (APN).
regex	Prevents the filtering of the APN address for the GNU regular expression (regex) matching library.
regex-parameter-map	Name of the APN regex parameter map.
mcc	Prevents the filtering of a valid mobile country code (MCC).
country-code	Mobile country code. The range is from 0 to 999.
mnc	Prevents the filtering of a mobile network code (MNC).
network-code	Mobile network code. The range is from 0 to 999.
message-id *id*	Prevents the filtering of the GTP message ID. The range is from 1 to 255.
message-length	Prevents the filtering of the GTP message length.
min *min-length*	Prevents the filtering of the minimum length, in bytes, of the GTP message. The range is from 1 to 65536.
max *max-length*	Prevents the filtering of the maximum length, in bytes, of the GTP message. The range is from 1 to 65536.
version *number*	Prevents the filtering of the GTP version. Valid values are 0 and 1.

Command Default

No classification criteria are negated.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

When you configure the **match not** command, the specified criteria is not matched.

The **mcc** *country-code* and **mnc** *network-code* keyword-argument combinations are used for International Mobile Subscriber Identity (IMSI) prefix filtering, where the country code contains three digits and the network code contains two or three digits.

The **message-length** keyword allows you to filter packets that do not meet the configured maximum and minimum length values. The message length is the sum of the GTP header and the rest of the message such as the payload of a UDP packet.

Examples

The following example shows how to negate the match criteria for a message with a minimum length of 300 bytes and a maximum length of 500 bytes for GTPv0 inspect-type class map.

```
Device(config)# class-map type inspect gtpv0 layer7-cmap
Device(config-cmap)# match not message-length min 300 max 500
```

Related Commands

Command	Description
class-map type inspect	Creates an application-specific inspect-type class map and enters QoS class-map configuration mode.
match (GTP)	Configures the classification criteria for a GTP inspect-type class map.

match program-number

To specify the allowed Remote Procedure Call (RPC) protocol program number as a match criterion, use the **match program-number** command in class-map configuration mode. To disable this match criterion, use the **no** form of this command.

match program-number *program-number*

no match program-number *program-number*

Syntax Description

program-number	Allowed program number.

Command Default

Disabled

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This match criterion is allowed only for SUN Remote Procedure Call (SUNRPC) class maps. You can use the **match program-number** command only after specifying the **class-map type inspect sunrpc**command.

Examples

The following example configures the program number 2345 as a match criterion in the class map rpc-prog-nums:

```
class-map type inspect sunrpc rpc-prog-nums
 match program-number 2345
```

Related Commands

Command	Description
class-map type inspect sunrpc	Configures inspection parameters for SUNRPC.
ip inspect name	Defines a set of inspection rules.

match protocol (zone)

To configure a match criterion for a class map on the basis of the specified protocol, use the **match protocol** command in class-map configuration mode. To remove the protocol-based match criterion from a class map, use the **no** form of this command.

match protocol *protocol-name* [*parameter-map*] **[signature]**

no match protocol *protocol-name* [*parameter-map*] **[signature]**

Syntax Description

protocol-name	Name of the protocol used as a matching criterion. For a list of supported protocols, use the CLI help option (**?**) on your platform.
parameter-map	(Optional) Protocol-specific parameter map.
signature	(Optional) Enables signature-based classification for peer-to-peer (P2P) packets. **Note** This option is available only for P2P traffic.

Command Default

No protocol-based match criterion is configured for a class map.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(6)T	This command was introduced for the zone-based policy firewall.
12.4(9)T	This command was modified. Support for the following protocols was added: • P2P protocols: **bittorrent**, **directconnect**, **edonkey**, **fasttrack**, **gnutella**, **kazaa2**, and **gtpv0**, **gtpv1**, **winmx** • Instant Messenger (IM) protocols: **aol**, **msnmsgr**, and **ymsgr** Also, the **signature** keyword was added to be used only with P2P protocols.
12.4(11)T	This command was modified. Support for the H.225 Remote Access Services (RAS) protocol and the **h225ras** keyword was added.

Release	Modification
12.4(20)T	This command was modified. Support for the I Seek You (ICQ) and Windows Messenger IM protocols and the following keywords was added: **icq**, **winmsgr**. Support for the H.323 protocol and the **h323** keyword was added. Support for the Session Initiation Protocol (SIP) and the **sip** keyword was added.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.0(1)M	This command was modified. The **extended** keyword was removed from the protocol name.
15.1(1)T	This command was modified. Support for the CU-SeeMe protocol and **cuseeme** keyword was removed.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. The following keywords were added: **netbios-dgm**, **netbios-ns**, and **netbios-ssn**.
Cisco IOS XE Release 3.4S	This command was modified. Support for the GPRS Tunneling Protocol (GTP) and **gtpv0** and **gtpv1** keywords was added.

Usage Guidelines

Use the **match protocol** command to specify the traffic based on a particular protocol. You can use this command in conjunction with the **match access-group** and **match class-map** commands to build sophisticated traffic classes.

The **match protocol** command is available under the **class-map type inspect** command.

If you enter the **match protocol** command under the **class-map type inspect** command, the Port to Application Mappings (PAM) are honored when the protocol field in the packet is matched against the command. All port mappings configured in the PAM table appear under the class map.

When packets are matched to a protocol, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

In Cisco IOS Release 12.4(15)T, if Simple Mail Transfer Protocol (SMTP) is currently configured for inspection in a class map and the inspection of Extended SMTP (ESMTP) needs to be configured, then the **no match protocol smtp** command must be entered before adding the **match protocol smtp extended** command. To revert to regular SMTP inspection, use the **no match protocol smtp extended** command, and then enter the **match protocol smtp** command. If these commands are not configured in the proper order, the following error is displayed:

%Cannot add this filter. Remove match protocol smtp filter and then add this filter.

In Cisco IOS Release 15.0(1)M and later releases, the **extended** keyword was removed from the **match protocol smtp** command.

Examples

The following example shows how to specify a class map called c1 and configure the HTTP protocol as a match criterion:

```
class-map type inspect c1
 match protocol http
```

The following example shows how to specify different class maps for ICQ and Windows Messenger IM applications:

```
! Define the servers for ICQ.
parameter-map type protocol-info icq-servers
 server name *.icq.com snoop
 server name oam-d09a.blue.aol.com
! Define the servers for Windows Messenger.
parameter-map type protocol-info winmsgr-servers
 server name messenger.msn.com snoop

! Define servers for yahoo.
parameter-map type protocol-info yahoo-servers
 server name scs*.msg.yahoo.com snoop
 server name c*.msg.yahoo.com snoop

! Define class-map to match ICQ traffic.
class-map type inspect icq-traffic
 match protocol icq icq-servers

! Define class-map to match windows Messenger traffic.
class-map type inspect winmsgr-traffic
 match protocol winmsgr winmsgr-servers
!

! Define class-map to match text-chat for windows messenger.
class-map type inspect winmsgr winmsgr-textchat
 match service text-chat
!

Define class-map to match default service
class-map type inspect winmsgr winmsgr-defaultservice
 match service any
!
```

The following example shows how to specify a class map called c1 and configure the netbios-dgm protocol as a match criterion:

```
class-map type inspect c1
 match protocol netbios-dgm
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 or Layer 4 inspect type class map.
match access-group	Configures the match criteria for a class map based on a specified ACL.
match protocol (zone)	Configures match criterion for a class map on the basis of a specified protocol.
parameter-map type protocol-info	Creates or modify a protocol-specific parameter map.

Command	Description
server	Associates a Diameter server with a Diameter authentication, authorization, and accounting (AAA) server group.

match protocol h323-annexe

To enable the inspection of H.323 protocol Annex E traffic which works on the User Datagram Protocol (UDP) diagnostic port or TCP port 2517, use the **match protocol h323-annexe** command in class-map configuration mode. To disable the inspection, use the **no** form of this command.

match protocol h323-annexe

no match protocol h323-annexe

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the match protocol h323-annexe command to inspect traffic based on Annex E of the H.323 protocol that uses the UDP diagnostic port or TCP port 2517. You can use this command in conjunction with the match access-group command to build sophisticated traffic classes.

The match protocol h323-annexe command is available under the class-map type inspect command.

Examples

The following example shows how to configure a voice policy to inspect the H.323 protocol Annex E packets for the "my-voice-class" class map.

```
class-map type inspect match-all my-voice-class
 match protocol h323-annexe
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
match access-group	Configures the match criteria for a class map based on the specified ACL.

Command	Description
match protocol h323-nxg	Enables the inspection of H.323 protocol Annex G traffic exchanged between border elements (BE) using the User Datagram Protocol (UDP) diagnostic port or TCP port 2099.

match protocol h323-nxg

To enable the inspection of H.323 protocol Annex G traffic exchanged between border elements (BE) using User Datagram Protocol (UDP) diagnostic port or TCP port 2099, use the **match protocol h323-nxg** command in class-map configuration mode. To disable the inspection, use the **no** form of this command.

match protocol h323-nxg

no match protocol h323-nxg

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the match protocol h323-nxg command to inspect traffic based on Annex G of the H.323 protocol that uses the UDP diagnostic port or TCP port 2099 to exchange traffic between border elements. You can use this command in conjunction with the match access-group command to build sophisticated traffic classes.

The match protocol h323-nxg command is available under the class-map type inspect command.

Examples

The following example shows how to configure a voice policy to inspect the H.323 protocol Annex G packets for the "my-voice-class" class map.

```
class-map type inspect match-all my-voice-class
 match protocol h323-nxg
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
match access-group	Configures the match criteria for a class map based on the specified ACL.

Command	Description
match protocol h323-annexe	Enables the inspection of H.323 protocol Annex E traffic which works on the UDP diagnostic port or TCP Port 2517.

match protocol-violation

To configure a Session Initiation Protocol (SIP) class map to use the protocol-violation method as a match criterion for permitting or denying SIP traffic, use the **match protocol-violation**command in class-map configuration mode. To remove the protocol-violation based match criterion from a class map, use the **no** form of this command.

match protocol-violation

no match protocol-violation

Syntax Description

This command has no arguments or keywords.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect**command.

Examples

The following example shows how to specify the protocol-violation method as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match protocol-violation
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match ra prefix-list

To verify the advertised prefixes in inspected messages from the authorized prefix list, use the **match ra prefix-list** command in RA guard policy configuration mode.

match ra prefix-list *ipv6-prefix-list-name*

Syntax Description

ipv6-prefix-list-name	The IPv6 prefix list to be matched.

Command Default

Advertised prefixes are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **match ra prefix-list** command enables verification of the advertised prefixes in inspected messages from the configured authorized prefix list. Use the **ipv6 prefix-list** command to configure an IPv6 prefix list. For instance, to authorize the 2001:101::/64 prefixes and deny the 2001:100::/64 prefixes, define the following IPv6 prefix list:

```
Router(config)# ipv6 prefix-list listname1 deny 2001:0DB8:101:/64
Router(config)# ipv6 prefix-list listname1 permit 2001:0DB8:100::/64
```

Examples

The following example shows how the command defines an router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and verifies the advertised prefixes in listname1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ra prefix-list listname1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.

match recipient address regex

To specify a non-existent e-mail recipient pattern in order to learn a spam sender and their domain information by luring them to use this contrived e-mail recipient, use the **match recipient address regex**command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match recipent address regex *parameter-map-name*

no match recipent addressregex*parameter-map-name*

Syntax Description

parameter-map-name	Specifies the name of the non-existent e-mail recipient pattern.

Command Default

The fictitious names of e-mail recipients are not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

A non-existent e-mail recipient pattern can be specified to learn about a spam sender and their domain information by luring them to use this non-existent e-mail recipient pattern. This pattern is a regular-expression (regex) that can be specified to identify an e-mail addressed to a particular recipient or domain when a server is functioning as a relay. The specified pattern is checked in the SMTP RCPT command (SMTP envelope) parameter to identify if the recipient is either used as an argument or a source-list to forward mail in the route specified in the list.

Note The **match recipient address regex** command does not operate on the ‘To’ or ‘Cc’ fields in the e-mail header.

Examples

The following example shows how to configure a regular expression non-existent e-mail recipient pattern:

```
parameter-map type regex known-unknown-users
 pattern “john@mydomain.com”
class-map type inspect smtp c1
 match recipient address regex known-unknown-users
policy-map type inspect smtp p1
```

```
class type inspect smtp c1
reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
parameter-map type regex	Enters the parameter-map name of a specific traffic pattern.
pattern	Cisco IOS regular expression (regex) pattern that matches the traffic pattern for the e-mail sender or user accounts from suspected domains that are causing the spam e-mail.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.
reset	(Optional) Drops an SMTP connection with an SMTP sender (client) if it violates the specified policy. This action sends an error code to the sender and closes the connection gracefully.

match recipient count gt

To specify an action that occurs when a number of invalid recipients appear on an SMTP connection, use the **match recipient count gt**command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match recipent count gt *value*

no match recipent countgt*value*

Syntax Description

value	Specifies the number of **RCPT** SMTP commands sent by the sender (client) to recipients who are specified in a single SMTP transaction to limit these commands.

Command Default

The number of RCPT SMTP commands sent by a sender to recipients is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

Spammers who search for a large number of user accounts in a domain typically send the same e-mail to all the user accounts they find in this domain. Spammers can be identified and restricted from searching for user accounts in a domain by using the **match recipient count gt** command.

Note The **match recipient count gt** command does not count the number of recipients specified in the 'To:' or 'Cc:' fields in the e-mail header.

Examples

The following example shows how to configure an SMTP application firewall policy to determine the number of **RCPT** lines and invalid recipients, for which the server has replied "500 No such address," in the SMTP transaction:

```
class-map type inspect smtp c1
 match recipient count gt 25
policy-map type inspect smtp p1
```

```
class type inspect smtp c1
reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.
reset	(Optional) Drops an SMTP connection with an SMTP sender (client) if it violates the specified policy. This action sends an error code to the sender and closes the connection gracefully.

match recipient invalid count gt

To identify and restrict the number of invalid SMTP recipients that can appear in an e-mail from senders who try common names on a domain in the hope that they discover a valid user name to whom they can send spam, use the **match recipient invalid count gt** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match recipent invalid count gt *value*

no match recipent invalid countgt*value*

Syntax Description

value	Specifies a maximum number of invalid e-mail recipients on this SMTP connection.

Command Default

The a number of invalid e-mail recipients is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

If a sender specifies in an invalid e-mail recipient and SMTP encounters this invalid recipient on the SMTP connection, then SMTP sends an error code reply to the e-mail sender (client) to specify another recipient. In this case, the event did not violate the SMTP protocol or indicate that this particular SMTP connection is bad. However, if a pattern of invalid recipients appears, then a reasonable threshold can be set to restrict these nuisance SMTP connections.

Examples

The following example shows how to configure an SMTP application firewall policy that restricts the number of invalid e-mail recipients on this SMTP connection to 5:

```
class-map type inspect smtp c1
 match recipient invalid count gt 5
policy-map type inspect smtp p1
 class type inspect smtp c1
 reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.
reset	(Optional) Drops an SMTP connection with an SMTP sender (client) if it violates the specified policy. This action sends an error code to the sender and closes the connection gracefully.

match reply ehlo

To identify and mask a service extension parameter in the EHLO server reply (e.g. 8BITMIME, ETRN) to prevent a sender (client) from using that particular service extension, use the **match reply ehlo**command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match reply ehlo {*parameter*| *WORD*}

nomatch reply ehlo {*parameter*| *WORD*}

Syntax Description

parameter	Specify a parameter from the well-known EHLO keywords.
WORD	Specify an extension which is not on the EHLO list (e.g. private extension XFOOBAR). Non-alphanumeric characters, such as hyphens, are not supported.

Command Default

The service extension parameter in the EHLO server reply is not defined or masked.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following example shows how to configure an SMTP application firewall policy that identifies and masks a well-known service extension parameter in the EHLO server reply:

```
class-map type inspect smtp c1
 match reply ehlo ETRN
policy-map type inspect smtp p1
 class type inspect smtp c1
 log
 mask
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
class type inspect smtp	Configures an SMTP class-map firewall for SMTP inspection parameters.
log	Logs an action related to this class-type in the SMTP policy map.
mask (policy-map)	Explicitly masks specified SMTP commands or the parameters returned by the server in response to an EHLO command.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map.

match req-resp

To configure a Session Initiation Protocol (SIP) class map to use the req-resp methods as a match criterion for permitting or denying SIP traffic, use the **match req-resp** command in class-map configuration mode. To remove the req-resp based match criterion from a class map, use the **no** form of this command.

match req-resp header *field* **regex** *regex-parameter-map*

no match req-resp header *field* **regex** *regex-parameter-map*

Syntax Description

header	Identifies the SIP header field.
field	Name of the request header field. The following are valid request header fields: **accept**, **accept-encoding**, **accept-language**, **alert-info**, **allow**, **contact**, **content-disposition**, **content-encoding**, **content-language**, **content-length**, **content-type**, **from**, **record-route**, **supported**, **to**, **user-agent**, **via**.
regex	Indicates that a regular expression will follow.
regex-parameter-map	Configures a parameter map of type **regex**.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect**command.

Examples

The following example shows how to specify the req-resp method as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match req-resp header via regex unsecure_proxy
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match req-resp body length

To configure an HTTP class map to use the minimum or maximum message size, in bytes, as a match criterion for permitting or denying HTTP traffic through the firewall, use the **match req-resp body length** command in class-map configuration mode. To remove message-size limitations from your configuration, use the **no** form of this command.

match req-resp body length {**lt** *bytes*| **gt** *bytes*}

no match req-resp body length {**lt** *bytes*| **gt** *bytes*}

Syntax Description

lt *bytes*	Minimum number of bytes in each message. The range is from 0 to 65535.
gt *bytes*	Message cannot be greater than the specified number of bytes.

Command Default

Message size is not considered when permitting or denying HTTP messages.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map,only after entering the **class-map type inspect http** command.

If the message body length is less than or greater than the specified values, a match occurs.

Examples

The following example, which shows how to define the HTTP application firewall policy http-class, will not permit HTTP messages longer than 1 byte:

```
class-map type inspect http http-class
 match req-resp body length 1
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

match req-resp header content-type

To match traffic based on the content type of the HTTP body, use the **match req-resp header content-type** command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match req-resp header content-type {**violation| mismatch| unknown**}

no match req-resp header content-type {**violation| mismatch| unknown**}

Syntax Description

violation	Flags a match if the content-type definition and the content type of the actual body do not match.
mismatch	Verifies the content-type of the response message against the accept field value of the request message.
unknown	Flags a match when an unknown content-type is found.

Command Default

No content-type checking is performed.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use the **match req-resp header content-type**command when you are configuring an HTTP firewall policy map, only after entering the **class-map type inspect http** command.

The **match req-resp header content-type**command configures a policy based on the content type of HTTP traffic. The command verifies that the header is one of the following supported content types:

- audio/*
- audio/basic
- audio/midi
- audio/mpeg
- audio/x-adpcm
- audio/x-aiff

- audio/x-ogg
- audio/x-wav
- application/msword
- application/octet-stream
- application/pdf
- application/postscript
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/x-gzip
- application/x-java-arching
- application/x-java-xm
- application/zip
- image/*
- image/cgf
- image/gif
- image/jpeg
- image/png
- image/tiff
- image/x-3ds
- image/x-bitmap
- image/x-niff
- image/x-portable-bitmap
- image/x-portable-greymap
- image/x-xpm
- text/*
- text/css
- text/html
- text/plain
- text/richtext
- text/sgml
- text/xmcd
- text/xml
- video/*

- video/-flc
- video/mpeg
- video/quicktime
- video/sgi
- video/x-avi
- video/x-fli
- video/x-mng
- video/x-msvideo

Examples

The following example configures an HTTP class map based on the content type of HTTP traffic:

```
class-map type inspect http http-class
 match req-resp header content-type unknown
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
content-type-verification	Permits or denies HTTP traffic through the firewall on the basis of content message type.
content-type-verification-match-req-rsp	Verifies the content type of the HTTP response against the accept field of the HTTP request.

match req-resp header transfer-encoding

To permit or deny HTTP traffic according to the specified transfer encoding of the message, use the **match req-resp header transfer-encoding**command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match req-resp header transfer-encoding {**chunked**| **compress**| **deflate**| **gzip**| **identity**| **all**}

no match req-resp header transfer-encoding {**chunked**| **compress**| **deflate**| **gzip**| **identity**| **all**}

Syntax Description

chunked	Encoding format (specified in RFC 2616, Hypertext Transfer Protocol--HTTP/1) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
compress	Encoding format produced by the UNIX compress utility.
deflate	ZLIB format defined in RFC 1950, ZLIB Compressed Data Format Specification Version 3.3, combined with the deflate compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification Version 1.3.
gzip	Encoding format produced by the gzip (GNU zip) program.
identity	Default encoding, which indicates that no encoding has been performed.
all	All of the transfer encoding types.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map, after entering the **class-map type inspect http** command.

Examples

The following example permits or denies HTTP traffic according to the encoding format produced by the UNIX compress utility:

```
class-map type inspect http http-class
 match req-resp header transfer-encoding compress
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
transfer-encoding type	Permits or denies HTTP traffic according to the specified transfer-encoding of the message.

match req-resp protocol-violation

To allow HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected, use the **match req-resp protocol-violation**command in class-map configuration mode. To disable configured settings, use the **no** form of this command.

match req-resp protocol-violation

no match req-resp protocol-violation

Syntax Description

This command has no arguments or keywords.

Command Default

All traffic is allowed through the firewall.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map, after entering the **class-map type inspect http** command.

The **match req-resp protocol-violation**command allows HTTP messages to pass through the firewall, If desired, in the policy map you can reset the TCP connection when HTTP noncompliant traffic is detected.

Examples

The following example allows HTTP messages to pass through the firewall:

```
class-map type inspect http http-class
 match req-resp protocol-violation
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

match request

To configure a Session Initiation Protocol (SIP) class map to use the request methods as a match criterion for permitting or denying SIP traffic, use the **match request** command in class-map configuration mode. To remove request based match criterion from a class map, use the **no** form of this command.

match request {**method** *method-name*| **header** *field* **regex** *regex-parameter-map*}

no match request {**method** *method-name*| **header** *field* **regex** *regex-parameter-map*}

Syntax Description

method	Identifies the SIP request method.
method-name	Name of the method (for example, **ack**) used as a matching criterion. See the "Usage Guidelines" for a list of methods supported by most routers.
header	Identifies the SIP header field.
field	Name of the request header field. The following are valid request header fields: **accept**, **accept-encoding**, **accept-language**, **alert-info**, **allow**, **authorization**, **contact**, **content-disposition**, **content-encoding**, **content-language**, **content-length**, **content-type**, **from**, **in-reply-to**, **max-forwards**, **priority**, **proxy-authorization**, **proxy-require**, **record-route**, **route**, **subject**, **supported**, **to**, **user-agent**, **via**, **warning**.
regex	Indicates that a regular expression will follow.
regex-parameter-map	Configures a parameter map of type **regex**.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect**command.

Supported Methods

The table below lists the request methods supported by most routers. For a complete list of supported methods, see the online help for the **match request** command on the router that you are using.

Table 1: Supported Methods

Method Name	Description
ack	Acknowledges that the previous message is valid and accepted.
bye	Signifies intent to terminate a call.
cancel	Terminates any pending request.
info	Communicates midsession signaling information along the signaling path for a call.
invite	Sets up a call.
message	Sends an instant message.
notify	Informs subscribers of state changes.
options	Allows a user-agent (UA) to query another UA or a proxy server about its capabilities.
prack	Provides reliable transfer of provisional response messages.
refer	Indicates that the recipient should contact a third party using the contact information provided in the request.
register	Includes a contact address to which SIP requests for the address-of-record should be forwarded.
subscribe	Requests state subscription. It is a dialog creating method.
update	Allows a client to update the parameters of a session (for example, the set of media streams and their codecs), but has no impact on the state of a dialog.

Examples

The following example shows how to specify the request method **subscribe** as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match request method subscribe
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match request length

To configure an HTTP firewall policy to use the uniform resource identifier (URI) or argument length in the request message as a match criterion for permitting or denying HTTP traffic, use the **match request length** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match request {**uri**| **arg**} **length gt** *bytes*

no match request {**uri**| **arg**} **length gt** *bytes*

Syntax Description

uri | **arg**	Firewall will search the URI or argument length of the request message as the match criterion.
gt *bytes*	Permits HTTP traffic if the URL in the request message contains more than the specified number of bytes.

Command Default

URI or argument lengths are not considered when permitting or denying HTTP traffic.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **arg** keyword was added.

Usage Guidelines

Use the **match request length** command to verify the length of the URI or argument that is being sent in a request message and apply the configured action when the length exceeds the configured threshold.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an HTTP application firewall policy to raise an alarm whenever the URI length of a request message exceeds 3076 bytes:

```
class-map type inspect http uri_len_cm
 match request uri length gt 3076
policy-map type inspect http uri_len_pm
 class type inspect http uri_len_cm
log
```

The following example shows how to configure an HTTP application firewall policy to raise an alarm whenever the argument length of a request message exceeds 512 bytes.

```
class-map type inspect http arg_len_cm
 match request arg length gt 512
policy-map type inspect http arg_len_pm
 class type inspect http arg_len_cm
 log
```

match request method

To configure an HTTP class map to use the request methods or the extension methods as a match criterion for permitting or denying HTTP traffic, use the **match request method** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match request method {**connect**| **copy**| **delete**| **edit**| **get**| **getattribute**| **getattributenames**| **getproperties**| **head**| **index**| **lock**| **mkdir**| **move**| **options**| **post**| **put**| **revadd**| **revlabel**| **revlog**| **revnum**| **save**| **setattribute**| **startrev**| **stoprev**| **trace**| **unedit**| **unlock**}

no match request method {**connect**| **copy**| **delete**| **edit**| **get**| **getattribute**| **getattributenames**| **getproperties**| **head**| **index**| **lock**| **mkdir**| **move**| **options**| **post**| **put**| **revadd**| **revlabel**| **revlog**| **revnum**| **save**| **setattribute**| **startrev**| **stoprev**| **trace**| **unedit**| **unlock**}

Syntax Description

connect	Connect method.
copy	Copy extension method.
delete	Delete method.
edit	Edit extension method.
get	Get method.
getattribute	Getattribute extension method.
getattributenames	Getattributenames extension method.
getproperties	Getproperties method.
head	Head method.
index	Index extension method.
lock	Lock extension method.
mkdir	Mkdir extension method.
move	Move extension method.
options	Options method.
post	Post method.
put	Put method.
revadd	Revadd extension method.

revlabel	Revlabel extension method.
revlog	Revlog extension method.
revnum	Revnum extension method.
save	Save extension method.
setattribute	Setattribute extension method.
startrev	Startrev extension method.
stoprev	Stoprev extension method.
trace	Trace method.
unedit	Unedit extension method.
unlock	Unlock extension method.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall class map, after entering the **class-map type inspect http** command.

Examples

The following example specifies that the match criteria is connect:

```
class-map type inspect http http-class
 match request method connect
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

match request not regex

To negate a match result in a HTTP firewall policy, use the **match request not regex**command in class-map configuration mode. To reset the match criterion, use the **no** form of this command.

match request not uri regex *parameter-map-name*

no match request not uri regex *parameter-map-name*

Syntax Description

uri	Firewall policy will search the URI or argument as the match criterion.
parameter-map-name	HTTP-based parameter map as specified via the **parameter-map type** command.

Command Default

Match negation is not enabled.

Command Modes

Class-map configuration (config-cmap)#

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **match request not uri regex**command to negate a match result.

Examples

The following example shows how to negate a match result and the output of the configuration in the running configuration.

```
Router(config-cmap)#match not request uri regex pmap
Router(config-cmap)#match request method post
Router(config)#policy-map type inspect http httppmap
Route(config-pmap)# class type inspect http cmap
Router(config-pmap-c)reset
Router(config-pmap-c)log
```

In the following configuration, if the HTTP POST request does not match the URL regular expression, It will be classified under class 'httpcmap' and firewall will RESET the connection as it has RESET configured for this class.

```
parameter-map type regex pmap
 pattern .*Publications/OrderHardcopies/tabid/123/Default.aspx
class-map type inspect http match-all httpcmap
 match not request uri regex pmap
 match request method post
```

```
policy-map type inspect http pmap
 class type inspect http httpcmap
   reset
   log
 class class-default
```

Related Commands

Command	Description
parameter-map type	Defines a parameter map.
class-map type inspect	Defines an inspect type class map.
match request regex	Defines a HTTP firewall policy to permit or deny HTTP traffic.
policy-map type inspect	Defines an inspect type policy map.

match request port-misuse

To identify applications misusing HTTP port, use the **match request port-misuse** command in class-map configuration mode. To remove this inspection parameter, use the **no** form of this command.

match request port-misuse {**im**| **p2p**| **tunneling**| **any**}

no match request port-misuse {**im**| **p2p**| **tunneling**| **any**}

Syntax Description

im	Instant messaging protocol applications subject to inspection.
p2p	Peer-to-peer protocol applications subject to inspection.
tunneling	Tunneling applications subject to inspection: HTTPPort/HTTPHost.
any	Any type of misuse (**im**, **p2p**, and **tunneling**).

Command Default

Applications that are misusing the HTTP port cannot be identified.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **class-map type inspect http** command.

Examples

The following example identifies all types of misuse of the HTTP port:

```
class-map type inspect http http-class
 match request port-misuse any
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.

Command	Description
port-misuse	Permits or denies HTTP traffic through the firewall on the basis of specified applications in the HTTP message.

match request regex

To configure an HTTP firewall policy to permit or deny HTTP traffic on the basis of request messages whose uniform resource identifier (URI) or arguments (parameters) match a defined regular expression, use the **match request regex** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match request {**uri**| **arg**} **regex** *parameter-map-name*

no match request {**uri**| **arg**} **regex** *parameter-map-name*

Syntax Description

uri | **arg**	Firewall policy will search the URI or argument as the match criterion.
parameter-map-name	HTTP-based parameter map as specified via the **parameter-map type** command.

Command Default

URI or parameter matching is not enabled.

Command Modes

Class-map configuration (config-cmap)#

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(1)T	The **not** keyword was added.

Usage Guidelines

Use the **match request uri regex**command to block custom URLs and queries; use the **match request arg regex** command to block all messages whose parameters match the configured regular inspection.

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an HTTP application firewall policy to block any request whose URI matches any of the following regular expressions: ".*cmd.exe," ".*money," ".*gambling".

```
parameter-map type regex uri_regex_cm
 pattern ".*cmd.exe"
 pattern ".*money"
 pattern ".*gambling"
class-map type inspect http uri_check_cm
 match request uri regex uri_regex_cm
policy-map type inspect http uri_check_pm
```

```
 class type inspect http uri_check_cm
 reset
```

The following example shows how to configure an HTTP application firewall policy to block any request whose arguments match the ".*codered" or the ".*attack" regular expressions:

```
parameter-map type regex arg_regex_cm
 pattern ".*codered"
 pattern ".*attack"
class-map type inspect http arg_check_cm
 match request arg regex arg_regex_cm
policy-map type inspect http arg_check_pm
 class type inspect http arg_check_cm
 reset
```

Related Commands

Command	Description
parameter-map type	Defines a parameter map.
class-map type inspect	Defines an inspect type class map.
policy-map type inspect	Defines an inspect type policy map.

match response

To configure a Session Initiation Protocol (SIP) class map to use a response method as the match criterion for permitting or denying SIP traffic, use the **match response** command in class-map configuration mode. To remove the response based match criterion from a class map, use the **no** form of this command.

match response {**header** *field*| **status**} **regex** *regex-parameter-map*

no match response {**header** *field*| **status**} **regex** *regex-parameter-map*

Syntax Description

header	(Optional) Identifies the SIP header field.
field	Name of the request header field. The following are valid request header fields: **accept**, **accept-encoding**, **accept-language**, **alert-info**, **allow**, **authentication-info**, **contact**, **content-disposition**, **content-encoding**, **content-language**, **content-length**, **content-type**, **error-info**, **from**, **proxy-authenticate**, **record-route**, **retry-after**, **server**, **supported**, **to**, **user-agent**, **via**, **www-authenticate**.
status	(Optional) Identifies status line in response.
regex	Indicates that a regular expression will follow.
regex-parameter-map	Name of parameter-map.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command when configuring an SIP firewall class map, after entering the **class-map type inspect**command.

Examples

The following example shows how to specify the response method as a match criterion.

```
Router(config)# class-map type inspect sip sip-class
Router(config-cmap)# match response status regex allowed-im-users
```

Related Commands

Command	Description
class-map type inspect sip	Creates a class map for SIP.

match response body java-applet

To identify Java applets in an HTTP connection., use the **match response body java-applet**command in class-map configuration mode. To remove this inspection rule, use the **no** form of this command.

match response body java-applet

no match response body java-applet

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command when you are configuring an HTTP firewall policy map, after entering the **class-map type inspect http** command.

Examples

The following example identifies Java applets in an HTTP connection:

```
class-map type inspect http http-class
 match response body java-applet
```

Related Commands

Command	Description
class-map type inspect http	Creates a class map for HTTP.
ip inspect name test http java-list	For Java applet blocking, specifies the numbered standard access list to use to determine friendly sites.

match response status-line regex

To specify a list of regular expressions that are to be matched against the status line of a response message, use the **match response status-line regex** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match response status-line regex *parameter-map-name*

no match response status-line regex *parameter-map-name*

Syntax Description

parameter-map-name	Name of parameter map.

Command Default

The status line of response messages is not considered when permitting or denying HTTP traffic.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If a match is found, possible actions that can be specified within the policy are as follows: allow, reset, or log. (The log action triggers a syslog message when a match is found.)

Examples

The following example shows how to configure an HTTP firewall policy to log an alarm whenever an attempt is made to access a forbidden page. (A forbidden page usually contains a 403 status-code and the status line looks like “HTTP/1.0 403 page forbidden\r\n”.)

```
parameter-map type regex status_line_regex
 pattern “[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403”
class-map type inspect http status_line_cm
 match response status-line regex status_line_regex
policy-map type inspect http status_line_pm
 class type inspect http status_line_cm
 log
```

match search-file-name

To use filenames within a search request as the match criterion, use the **match search-file-name**command in class-map configuration mode. To remove this match criterion from the configuration file, use the **no** form of this command.

match search-file-name [*regular-expression*]

no match search-file-name [*regular-expression*]

Syntax Description

regular-expression	(Optional) The regular expression used to identify specific filenames within a search request. For example, entering ".exe" as the regular expression would classify the filenames containing the string ".exe" as matches for the traffic policy. If this argument is not issued, all filenames are classified, as appropriate.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **match search-file-name**command to configure the Cisco IOS Firewall to block filenames within a search request for clients using the eDonkey peer-to-peer (P2P) protocol.

Note This command is available only for the eDonkey P2P protocol.

Examples

The following example shows how to configure a Cisco IOS Firewall to block filename searches for ".exe" and permit file transfers within the eDonkey protocol:

```
! Select eDonkey protocol requiring L7 policies
class-map type inspect match-any my-restricted-p2p
 match protocol edonkey signature
!
! Configure Edonkey to look for "*.exe" in searches
```

```
class-map type inspect edonkey my-edonkey-exe
 match search-file-name "*.exe"
!
! Configure Edonkey to look for file-transfers
class-map type inspect edonkey my-edonkey-file-tx
 match file-transfer *
!
! Configure P2P Layer 7 policy map
policy-map type inspect p2p my-p2p-policy
! class type inspect edonkey my-edonkey-exe
 reset
 class type inspect edonkey my-edonkey-file-tx
 allow
 log
!
!
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match security-group

To configure the match criteria for a class map on the basis of a source or destination Security Group Tag (SGT) number, use the **match security-group** command in class-map configuration mode. To remove source or destination SGT match criteria from a class map, use the **no** form of this command.

match security-group {**source** *sgt-number*| **destination** *sgt-number*}

no match security-group {**source** *sgt-number*| **destination** *sgt-number*}

Syntax Description

source	Specifies the source SGT used as the match criteria against which packets are checked to determine if they belong to this class.
destination	Specifies the destination SGT used as the match criteria against which packets are checked to determine if they belong to this class.
sgt-number	Number used to define the source or destination SGT.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

When packets are matched to a source or destination SGT, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

To use the **match security-group** command, you must first enter the **class-map type inspect** command to specify the name of the class whose match criteria you want to establish.

Examples

The following example specifies a class map named cmap-3 and configures the source and destination SGT numbers to be used as the match criterion for that class in order to configure a class map for classifying a Security Group Access (SGA) zone-based policy firewall network traffic.

```
Router(config)# class-map type inspect match-all cmap-3
Router(config-cmap)# match security-group source tag 100
```

```
Router(config-cmap)# match security-group destination tag 200
Router(config-cmap)# exit
Router# show policy-map type inspect zone-pair session
```

Related Commands

Command	Description
class-map inspect type	Creates a class map to be used for matching packets to a specified class.
class type inspect	Creates a Layer 3 or Layer 4 inspect type policy map.
inspect	Enables packet inspection.
policy-map type inspect	Creates a Layer 3 or Layer 4 inspect type policy map.
service-policy type inspect	Attaches a firewall policy map to the destination zone pair.
show policy-map type inspect zone-pair session	Displays the Cisco IOS stateful packet inspection sessions created because of the policy-map application on the specified zone pair.
zone-pair security	Creates a zone pair.

match sender address regex

To specify spam e-mail from suspected domains and user accounts to be restricted, use the **match sender address regex**command in class-map configuration mode. To disable this inspection parameter, use the **no** form of this command.

match sender address regex *parameter-map-name*

no match sender address regex *parameter-map-name*

Syntax Description

parameter-map-name	Specifies the parameter-map name class, which is the name of a specific traffic pattern. This pattern is a Cisco IOS regular expression (regex) pattern for a class-map.

Command Default

The parameter-map name class is not defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **match sender address regex** command helps to match the parameter-map name of a specific traffic pattern that specifies a sender domain or e-mail address in the SMTP traffic. The specified pattern is scanned in the parameter for the SMTP **MAIL FROM:** command.

Examples

The following example shows how to configure an SMTP application firewall policy to restrict an e-mail sender from a suspected domain:

```
parameter-map type regex bad-guys
 pattern “*deals\.com”
 pattern *crazyperson*@hotmail\.com
class-map type inspect smtp match-any c1
 match sender address regex bad-guys
policy-map type inspect smtp p1
 class type inspect smtp c1
 log
 reset
```

Related Commands

Command	Description
class-map type inspect smtp	Creates a class map for the SMTP protocol so that the match criteria is set to match criteria for this class map.
parameter-map type regex	Enters the parameter-map name of a specific traffic pattern.
pattern	Cisco IOS regular expression (regex) pattern that matches the traffic pattern for the e-mail sender or user accounts from suspected domains that are causing the spam e-mail.

match server-domain urlf-glob

To configure the match criteria for a local URL filtering class map on the basis of server domain name, use the **match server-domain urlf-glob** command in class-map configuration mode. To remove the domain name match criteria from a URL filtering class map, use the **no** form of this command.

match server-domain urlf-glob *parameter-map-name*

no match server-domain urlf-glob *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match server-domain urlf-glob**command specifies the server domain matches for local URL filtering. Typically, you use this command in two class maps: one to specify trusted domains and one to specify untrusted domains. You must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** commandand create the local filtering class with the **class-map type urlfilter** command before using this command, otherwise you will receive an error message.

Examples

The following example shows the configuration for trusted domains and untrusted domains:

```
parameter-map type urlf-glob trusted-domain-param
 pattern www.example.com
 pattern *.example1.com
class-map type urlfilter match-any trusted-domain-class
 match server-domain urlf-glob trusted-domain-param
parameter-map type urlf-glob untrusted-domain-param
 pattern www.example3.com
 pattern www.example4.com
class-map type urlfilter match-any untrusted-domain-class
 match server-domain urlf-glob untrusted-domain-param
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.
match url-keyword urlf-glob	Specifies the match criteria for a local URL keyword filter.
parameter-map type urlf-glob	Specifies the per-policy parameters for local URL filtering of trusted domains, untrusted domains, and URL keywords.

match server-response any

To configure the match criterion for a SmartFilter (N2H2) or Websense URL filtering class map, use the **match server-response any** command in class-map configuration mode. To remove the match criterion, use the **no** form of this command.

match server-response any

no match server-response any

Syntax Description

This command has no arguments or keywords.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **match server-response any**command to specify that any response from the SmartFilter or Websense server results in a match. Use this command after you have created a class map with the **class-map type urlfilter n2h2** or the **class-map type urlfilter websense** command:

Examples

The following example shows the configuration for a SmartFilter class:

```
class-map type urlfilter n2h2 match-any smartfilter-class
 match server-response any
```

The following example shows the configuration for a Websense class:

```
class-map type urlfilter websense match-any websense-class
 match server-response any
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to which a URL filtering policy applies.

match service

To specify a match criterion for any supported Instant Messenger (IM) protocol, use the **match service** command in class-map configuration mode. To remove the match criterion from the configuration file, use the **no** form of this command.

match service {**any**| **text-chat**}

no match service {**any**| **text-chat**}

Syntax Description

any	Matches any type of service within the given IM protocol with the exception of text chat messages.
text-chat	Matches packets for text chat messages.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	Support for I Seek You (ICQ) and Windows Messenger IM Protocols was added.

Usage Guidelines

Use the **match service** command to configure the Cisco IOS Firewall to create a match criterion on the basis of text chat messages or for any available service within a given IM protocol.

Before you can use the **match service** command, you must issue the **class-map type inspect** command and specify one of the following IM protocols: AOL, ICQ, MSN Messenger, Yahoo Messenger, and Windows Messenger.

Examples

The following example shows how to configure an AOL IM policy that permits text chat and blocks any MSN IM service:

```
class-map type inspect aol match-any l7cmap-service-text-chat
 match service text-chat
!
class-map type inspect msnmsgr match-any l7cmap-service-any
 match service any
! Allow text-chat, reset if any other service, alarm for both
policy-map type inspect im l7pmap
```

```
class type inspect aol l7cmap-service-text-chat
allow
log
!
class type inspect msnmsgr l7cmap-service-any
reset
log
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match start

Note Effective with Cisco IOS Release 15.2(4)M, the **match start** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3), use the **match start** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match start {**l2-start**| **l3-start**} **offset** *number* **size** *number* {**eq**| **neq**| **gt**| **lt**| **range** *range*| **regex** *string*} {*value* [*value2*]| [*string*]}

no match start {**l2-start**| **l3-start**} **offset** *number* **size** *number* {**eq**| **neq**| **gt**| **lt**| **range** *range*| **regex** *string*} {*value* [*value2*]| [*string*]}

Syntax Description

l2-start	Match criterion starts from the datagram header.
l3-start	Match criterion starts from the network header.
offset *number*	Match criterion can be made according to any aribitrary offset.
size *number*	Number of bytes in which to match.
eq	*Match criteria is met if the* packet is equal to the specified value or mask.
neq	*Match criteria is met if the* packet is not equal to the specified value or mask.
mask	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	*Match criteria is met if the* packet is greater than the specified value.
lt	*Match criteria is met if the* packet is less than the specified value.
range *range*	Match critera is based upon a lower and upper boundary protocol field range.
regex *string*	Match critera is based upon a string that is to be matched.

value	Value for which the packet must be in accordance with.

Command Default No match criteria are configured.

Command Modes Class-map configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).
Cisco IOS XE 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines To the match criteria that is to be used for flexible packet matching, you must first enter the**class-map** command to specify the name of the class whose match criteria you want to establish. Thereafter, you can enter one of the following commands:

- **match field** (which configures the match criteria for a class map on the basis of the fields defined in the protocol header description files [PHDFs])
- **match start** (which can be used if a PHDF is not loaded onto the router)

Examples The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start l3-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start l3-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start l3-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
```

```
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match field	Configures the match criteria for a class map on the basis of the fields defined in the PHDFs.

match text-chat

To use text chat messages as the match criterion, use the **match text-chat** command in class-map configuration mode. To remove the match criterion from the configuration file, use the **no** form of this command.

match text-chat [*regular-expression*]

no match text-chat [*regular-expression*]

Syntax Description

regular-expression	(Optional) The regular expression used to identify specific eDonkey text chat messages. For example, entering ".exe" as the regular expression would classify the eDonkey text chat messages containing the string ".exe" as matches for the traffic policy. To specify that all eDonkey text chat messages be identified by the traffic class, use an asterisk (*) as the regular expression.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **match text-chat**command to configure the Cisco IOS firewall to block text chat messages between clients using the eDonkey peer-to-peer (P2P) application.

Note This command is available only for the eDonkey P2P protocol.

Examples

The following example shows how to configure all text chat messages to be classified into the "my-edonkey-exe" class map:

```
class-map type inspect edonkey match-any my-edonkey-exe
 match text-chat
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.

match (fqdn acl)

To specify the URL to be associated with the URL profile that configures the SDP registrar to run HTTPS, use the **match url**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

match url *url*

no match url *url*

Syntax Description

url	Specifies the URL to be associated with the URL profile.

Command Default

No URL is associated with the URL profile.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **match url**command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.

Command	Description
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

match url category

To configure the match criteria for a Trend-Micro URL filtering class map on the basis of the specified URL category, use the **match url category**command in class-map configuration mode. To remove the URL category match criteria from a URL filtering class map, use the **no** form of this command.

match url category *category-name*

no match url category *category-name*

Syntax Description

category-name	Name of the URL category.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match url category**command specifies the name of the URL category to be used as the match criteria against which packets are checked to determine whether they belong to the class specified by the class map. Before you can use the **match url category**command, you must first use the **class-map type urlfilter**command to specify the name of the class whose match criteria you want to establish.

To display a list of supported URL categories, use the **match url category ?** command in class map configuration mode.

Examples

The following example specifies a class map for Trend Micro filtering called drop-category and configures the URL categories Gambling and Personals-Dating as match criteria:

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.

Command	Description
match url reputation	Specifies a match criterion for a URL filtering class map on the basis of URL reputation.

match url-keyword urlf-glob

To configure the match criteria for a local URL filtering class map on the basis of the URL keyword, use the **match url-keyword urlf-glob** command in class-map configuration mode. To remove the keyword match criteria from a URL filtering class map, use the **no** form of this command.

match url-keyword urlf-glob *parameter-map-name*

no match url-keyword urlf-glob *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match url-keyword urlf-glob** command specifies URL keyword matches for local URL filtering. Typically, you use this command to specify the URL keywords for which you want to block access. You must configure the **urlf-glob** keyword with the **parameter-map type urlf-glob** commandand create the local filtering class with the **class-map type urlfilter** command before using this command, otherwise you will receive an error message.

Examples

The following example shows the use of:

- The **parameter-map type urlf-glob** command to configure the the keyword matching patterns.
- The **class-map type urlfilter** command to create the local URL filtering class keyword class.
- The **match url-keyword urlf-glob** command to specify the matching criteria for the class.

```
parameter-map type urlf-glob keyword-param
 pattern example
 pattern www.example1
 pattern example3
class-map type urlfilter match-any keyword-class
 match url-keyword urlf-glob keyword-param
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.
match server-domain urlf-glob	Specifies the match criteria for a local domain name filter.
parameter-map type urlf-glob	Specifies the per-policy parameters for local URL filtering of trusted domains, untrusted domains, and URL keywords.

match url reputation

To configure the match criteria for a Trend-Micro URL filtering class map on the basis of the specified URL reputation, use the **match url reputation**command in class-map configuration mode. To remove the URL reputation match criteria from a URL filtering class map, use the **no** form of this command.

match url reputation *reputation-name*

no match url reputation *reputation-name*

Syntax Description

reputation-name	Name of the URL reputation.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **match url reputation**command specifies the name of the URL reputation to be used as a match criterion against which packets are checked to determine whether they belong to the class specified by the class map. Before you can use the **match url reputation**command, you must first use the **class-map type urlfilter**command to specify the name of the class whose match criteria you want to establish.

To display a list of supported URL reputations, use the **match url reputation ?** command in class map configuration mode.

Examples

The following example specifies a class map for Trend Micro filtering called drop-reputation and configures the URL reputations ADWARE and PHISHING as match criteria:

```
class-map type urlfilter trend match-any drop-reputation
 match url reputation ADWARE
 match url reputation PHISHING
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map to be used for matching packets to which a URL filtering policy applies.

Command	Description
match url category	Specifies a match criterion for a URL filtering class map on the basis of URL category.

match user-group

To configure the match criterion for a class map on the basis of the specified user group, use the **match user-group** command in class-map configuration mode. To remove user-group based match criterion from a class map, use the **no** form of this command.

match user-group *group-name*

no match user-group *group-name*

Syntax Description

group-name	Name of the user-group used as a matching criterion.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

To use the **match user-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Examples

The following example specifies a class map called ftp and configures the user-group as a match criterion:

```
Router(config)# class-map type inspect match-all auth_proxy_ins_cm
Router(config-cmap)# description
!
Inspect Type Class-map for auth_proxy_ug
!
Router(config-cmap)# match protocol telnet
Router(config-cmap)# match user-group auth_proxy_ug
Router(config-cmap)# exit
Router(config)# class-map type inspect match-all eng_group_ins_cm
Router(config-cmap)# description
!
Inspect Type Class-map for eng_group_ug
!
Router(config-cmap)# match protocol telnet
Router(config-cmap)# match user-group eng_group_ug
Router(config-cmap)# exit
Router(config)# class-map type inspect match-all manager_group_ins_cm
Router(config-cmap)# description

!
Inspect Type Class-map for manager_group_ug
!
```

```
Router(config-cmap)# match protocol ftp
Router(config-cmap)# match user-group manager_group_ug
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
user-group	Defines the user-group associated with the identity policy.

max-destination

To configure the maximum number of destinations that a firewall can track, use the **max-destination** command in profile configuration mode. To disable the configuration, use the **no** form of this command.

max-destination *number*

no max-destination *number*

Syntax Description

number	Maximum destination value. Valid values are from 1 to 4294967295.

Command Default

The maximum number of destinations that a firewall can track is not configured.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-zone** command before you can configure the **max-destination** command.

The firewall creates an entry for each destination to track the rate of TCP synchronization (SYN) flood packets arriving from a zone to a destination address. The number of entries that a firewall creates should be limited, so that these entries do not consume a lot of memory during a denial-of-service (DoS) attack. The **max-destination** command configures the maximum number of destinations that a firewall can track. When the maximum limit is reached, the SYN packets to a destination are dropped.

Examples

The following example shows how to set the maximum number of destinations that a firewall can track to 10000:

```
Router(config)# parameter-map type inspect-zone
Router(config-profile)# max-destination 10000
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect-zone	Configures a parameter map of type inspect zone and enters profile configuration mode.

max-header-length

To permit or deny HTTP traffic on the basis of the message header length, use the **max-header-length**command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

max-header-length request *bytes* **response** *bytes* **action** {**reset**| **allow**} **[alarm]**

no max-header-length request *bytes* **response** *bytes* **action** {**reset**| **allow**} **[alarm]**

Syntax Description

request *bytes*	Maximum header length, in bytes, allowed in the request message. Number of bytes range: 0 to 65535.
response *bytes*	Maximum header length, in bytes, allowed in the response message. Number of bytes range: 0 to 65535.
action	Messages that exceed the maximum size are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not issued, all traffic is permitted.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All message header lengths exceeding the configured maximum size will be subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

max-incomplete

To define the number of existing half-open sessions that will cause the Cisco IOS firewall to start and stop deleting half-open sessions, use the **max-incomplete** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

max-incomplete {**low** *number-of-connections*| **high** *number-of-connections*}

no max-incomplete {**low** *number-of-connections*| **high** *number-of-connections*}

Syntax Description

low *number-of-connections*	Minimum number of half-open sessions that will cause the Cisco IOS firewall to stop deleting half-open sessions. The default is unlimited.
high *number-of-connections*	Maximum number of half-sessions after which the Cisco IOS firewall will start deleting half-open sessions. The default is unlimited.

Command Default

The maximum number is unlimited and no half-open sessions are deleted.

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **max-incomplete**subcommand after you enter the **parameter-map type inspect** command.

Enter the **max-incomplete**command twice. The first command specifies a high number at which the system will start deleting half-open sessions. The second command specifies a low number at which the system will stop deleting half-open sessions.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to specify that the Cisco IOS firewall will stop deleting half-open sessions when there is a minimum of 800 half-open sessions and a maximum of 10000 half-open sessions:

```
parameter-map type inspect internet-policy
 max-incomplete high 10000
 max-incomplete low unlimited 800
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

max-incomplete (parameter-map type)

To configure the half-opened session limit for VPN routing and forwarding (VRF), use the **max-incomplete** command in parameter-map type inspect configuration mode. To disable the half-opened session limit configuration, use the **no** form of this command.

max-incomplete [**icmp**| **tcp**| **udp**] *number*

no max-incomplete[**icmp**| **tcp**| **udp**]*number*

Syntax Description

icmp	(Optional) Specifies the maximum half-opened Internet Control Message Protocol (ICMP) connections per VRF.
tcp	(Optional) Specifies the maximum half-opened TCP connections per VRF.
udp	(Optional) Specifies the maximum half-opened UDP connections per VRF.
number	Number of half-opened sessions per VRF. Valid values are from 1 to 4294967295.

Command Default

The number of half-opened sessions is unlimited.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect global** or **parameter-map type inspect-vrf** command before you configure the **max-incomplete** command.

A half-opened session is a session that has not reached the established state.

When you configure the **max-incomplete** command after configuring the **parameter-map type inspect global**, command, the half-opened session limit is configured for the global VRF table.

When the configured half-opened session limit is reached, new connections are dropped.

Examples

The following example shows how to configure the half-opened session limit to 3400 for the global VRF table:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# max-incomplete 3400
Router(config-profile)# end
```

The following example shows how to configure the half-opened limit to 2380 for per-VRF firewall sessions:

```
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# max-incomplete 2380
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.
parameter-map type inspect-vrf	Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode.

max-incomplete aggressive-aging

To configure the maximum number of half-opened firewall sessions and the aggressive aging of half-opened firewall sessions for VPN routing and forwarding (VRF), use the **max-incomplete aggressive-aging** command in parameter-map type inspect configuration mode. To disable the configuration, use the **no** form of this command.

max-incomplete *number* **aggressive-aging high** {*value* **low** *value*| **percent** *percent* **low percent** *percent*}

no max-incomplete *number* **aggressive-aging high** {*value* **low** *value*| **percent** *percent* **low percent** *percent*}

Syntax Description

number	Number of half-opened sessions. Valid values are from 1 to 4294967295.
high	Specifies the high watermark for aggressive aging.
value	High watermark in absolute values. Valid values are from 1 to 4294967295.
low	Specifies the low watermark for aggressive aging.
value	Low watermark in absolute values. Valid values are from 1 to 4294967295.
percent *percent*	Specifies the high watermark percentage for aggressive aging. Valid values are from 1 to 100.
low percent *percent*	Specifies the low watermark percentage for aggressive aging. Valid values are from 1 to 100.

Command Default

The aggressive aging of half-opened sessions is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The Aggressive Aging feature allows the firewall to aggressively age out sessions to make space for new sessions, thereby protecting the firewall session table from filling.

A half-opened session is a session that has not reached the established state.

You must configure the **parameter-map type inspect global** or the **parameter-map type inspect-vrf** command before configuring the **max-incomplete aggressive-aging** command.

Examples

The following example shows how to configure the aggressive aging of half-opened sessions for a VRF:

```
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# max-incomplete 2345 aggressive-aging high percent 70 low percent
30
Router(config-profile)# end
```

Related Commands

Command	Description
max-incomplete (inspect-vrf)	Configures the half opened session limit for a VRF.
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.
parameter-map type inspect-vrf	Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode.

max-logins

To limit the number of simultaneous logins for users in a specific server group, use the **max-logins** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-logins *number-of-users*

no max-logins *number-of-users*

Syntax Description

number-of-users	Number of logins. The value ranges from 1 through 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of simultaneous logins for users in that group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of logins for users in server group “cisco” has been set to 8:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-logins 8
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-users	Limits the number of connections to a specific server group.

max-request

To specify the maximum number of outstanding requests that can exist at any given time, use the **max-request** command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

max-request *number-of-requests*

no max-request *number-of-requests*

Syntax Description

number-of-requests	Maximum number of pending requests that can be queued to the urlfiltering server.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **max-request**subcommand after you enter the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Examples

The following example specifies that there can be a maximum of 80 outstanding requests at a given time:

```
parameter-map type urlfilter u1
 max-request 80
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

max-resp-pak

To specify the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer, use the **max-resp-pak**command in URL parameter-map configuration mode. To disable this feature, use the **no** form of this command.

max-resp-pak *number-of-responses*

no max-resp-pak *number-of-responses*

Syntax Description

number-of-responses	Maximum number of HTTP responses that the firewall can keep in its packet buffer before it starts dropping responses.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **max-resp-pak**subcommand after you enter the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Examples

The following example specifies that there can be a maximum of 200 HTTP responses in the packet buffer:

```
parameter-map type urlfilter eng-filter-profile
 max-resp-pak 200
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

max-retry-attempts

To set the maximum number of retries before Single SignOn (SSO) authentication fails, use the **max-retry-attempts** command in webvpn sso server configuration mode. To remove the number of retries that were set, use the **no** form of this command.

max-retry-attempts *number-of-retries*

no max-retry-attempts *number-of-retries*

Syntax Description

number-of-retries	Number of retries. Value = 1 through 5. Default = 3.

Command Default

A maximum number of retries is not set. If this command is not configured, the default is 3 retries.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

Examples

The following example shows that the maximum number of retries is 3:

```
webvpn context context1
 sso-server test-sso-server
  max-retry-attempts 3
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

max-uri-length

To permit or deny HTTP traffic on the basis of the uniform resource identifier (URI) length in the request message, use the **max-uri-length**command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

max-uri-length *bytes* **action** {**reset**| **allow**} **[alarm]**

no max-uri-length *bytes* **action** {**reset**| **allow**} **[alarm]**

Syntax Description

bytes	Number of bytes ranging from 0 to 65535.
action	Messages that exceed the maximum URI length are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not issued, all traffic is permitted.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All URI lengths exceeding the configured value will be subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
```

```
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

max-users

To limit the number of connections to a specific server group, use the **max-users** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-users *number-of-users*

no max-users *number-of-users*

Syntax Description

number-of-users	Number of users. The value ranges from 1 through 5000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of connections to server group “cisco” has been set to 1200:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-users 1200
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-logins	Limits the number of simultaneous logins for users in a specific server group.

max-users (WebVPN)

To limit the number of connections to an SSL VPN that will be permitted, use the **max-users** command in webvpn context configuration mode. To remove the connection limit from the SSL VPN context configuration, use the **no** form of this command.

max-users *number*

no max-users

Syntax Description

number	Maximum number of SSL VPN user connections. A number from 1 to 1000 can be entered for this argument.

Command Default

The following is the default if this command is not configured or if the **no** form is entered:

number : 1000

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures a limit of 500 user connections that will be accepted by the SSL VPN:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# max-users 500
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

message retry count

To configure the number of times that a Trusted Information Distribution Protocol (TIDP) message is transmitted, use the **message retry count** command in parameter-map configuration mode. To configure TMS to use the default message timer value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **message retry count** command is not available in Cisco IOS software.

message retry count *number*

no message retry count *number*

Syntax Description

number	Number of times that a TMS message is retransmitted. A number from 0 through 5 is entered.

Command Default

The following default value is used if this command is not configured or if the **no** form is entered:

3

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The message timer regulates the number of times that the controller sends a Control Information Message (CIM) to a nonresponsive consumer.

Examples

The following example configures a controller to send messages to consumers up to 5 times at 15-second intervals:

```
Router(config)# parameter-map type tms TMS_PAR_1

Router(config-profile)# logging tms events
Router(config-profile)# heartbeat retry interval 60
Router(config-profile)# heartbeat retry count 3
Router(config-profile)# message retry interval 15
```

```
Router(config-profile)# message retry count 5
Router(config-profile)# exit
```

Related Commands

Command	Description
parameter-map type tms	Configures a TMS type parameter map.

message retry interval

To configure the time interval between the transmission of Transitory Messaging Services (TMS) messages, use the **message retry interval** command in parameter-map configuration mode. To configure TMS to use the default message timer value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **message retry interval** command is not available in Cisco IOS software.

message retry interval *time*

no message retry interval *time*

Syntax Description

time	The time interval, in seconds, between the transmission of TMS messages. A number from 3 through 300 is entered.

Command Default

The following default value is used if this command is not configured or if the **no** form is entered:

10

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The message timer regulates the number of times that the controller sends a Threat Information Message (TIM) to a nonresponsive consumer.

Examples

The following example configures a controller to send messages to consumers up to five times at 15-second intervals:

```
Router(config)# parameter-map type tms TMS_PAR_1
Router(config-profile)# logging tms events

Router(config-profile)# heartbeat retry interval 60
Router(config-profile)# heartbeat retry count 3
```

```
Router(config-profile)# message retry interval 15

Router(config-profile)# message retry count 5
Router(config-profile)# exit
```

Related Commands

Command	Description
parameter-map type tms	Configures a TMS type parameter map.

mime-type

To specify the Multipurpose Internet Mail Extensions (MIME) type that the SDP registrar should use to respond to a request received through the URL profile, use the **mime-type** command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

mime-type *mime-type*

no mime-type *mime-type*

Syntax Description

mime-type	Specifies the MIME type.

Command Default

No MIME type is configured for the SDP registrar.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **mime-type**command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.

Command	Description
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
match url	Specifies the URL to be associated with the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

mitigation through outgoing

mitigation

To specify the Transitory Messaging Services (TMS) parameter map associated with this TMS class, use the **mitigation** command in policy-map class configuration mode. To detach the parameter map from the policy map, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **mitigation** command is not available in Cisco IOS software.

mitigation *parameter-map-name*

no mitigation *parameter-map-name*

Syntax Description

parameter-map-name	Name of a TMS parameter map.

Command Default

None.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **mitigation** command is entered in policy-map class configuration mode to attach a TMS type parameter map to a TMS type class map under a policy map. The same parameter map can be attached to one or more class maps. If there are multiple class maps attached to a policy map, each can be associated with the same parameter map or a different parameter map.

Examples

The following example configures the **mitigation** command to attach the TMS type parameter map to the policy map:

```
Router(config)# class-map type control tms TMS_CLASS_1
Router(config-cmap)# match tidp-group 10-20
Router(config-cmap)# exit
Router(config)# parameter-map type tms TMS_PAR_1
router(config-profile)# controller ipv4 10.1.1.1
Router(config-profile)# exit
Router(config)# policy-map type control tms TMS_POL_1
```

```
Router(config-pmap)# class TMS_CLASS_1
Router(config-pmap-c)# mitigation TMS_PAR_1
Router(config-pmap-c)# end
```

Related Commands

Command	Description
policy-map type tms	Configures a TMS type policy map.

mls acl tcam consistency enable

To enable consistency checking of a device's Ternary Content Addressable Memory (TCAM) table by the Multi-Link Switching (MLS) access check list (ACL) lookup engine, use the **mls acl tcam consistency enable** command in global configuration mode. To return to the default value, use the **no** form of this command.

mls acl tcam consistency enable

Syntax Description

This command has no arguments or keywords.

Command Default

The MLS ACL TCAM consistency checker is disabled after a device reloads.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(1)S	This command was introduced.

Usage Guidelines

Use this command to explicitly enable the MLS ACL TCAM consistency checker.

To display the results from the consistency checker, use the **show mls acl consistency** command.

Examples

```
Device (config)# mls acl tcam consistency enable
Device(config)# exit
Device# show running-config
.
.
.
mls acl tcam consistency enable
mls cef error action freeze
multilink bundle-name authenticated
!
```

Related Commands

Command	Description
show mls acl consistency	Displays results from the MLS TCAM ACL consistency checker.

mls acl tcam default-result

To set the default action during the ACL TCAM update, use the **mls acl tcam default-result** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls acl tcam default-result {**permit**| **deny**| **bridge**}

no mls acl tcam default-result

Syntax Description

permit	Permits all traffic.
deny	Denies all traffic.
bridge	Bridges all Layer 3 traffic up to MSFC, RP, or to software.

Command Default

deny

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

In the transition time between when an existing ACL is removed and a new ACL is applied, a default **deny** is programmed in the hardware. Once the new ACL has been applied completely in the hardware, the default **deny** is removed.

Use the **mls acl tcam default-result permit** command to permit all traffic in the hardware or bridge all traffic to the software during the transition time.

Examples

This example shows how to permit all traffic to pass during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result permit
```

This example shows how to deny all traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result deny
```

This example shows how to bridge all Layer 3 traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result bridge
```

mls acl tcam override dynamic dhcp-snooping

To allow web-based authentication (webauth) and IP Source Guard (IPSG) to function together on the same interface, use the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode. To disable this compatibility function, use the **no** form of this command.

mls acl tcam override dynamic dhcp-snooping

no mls acl tcam override dynamic dhcp-snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This function is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI2	This command was introduced.

Usage Guidelines

On the Catalyst 6500 series switch, when both webauth and IPSG are configured on the same access port and DHCP snooping is enabled on the access VLAN, the webauth downloadable ACLs (DACLs) can interfere with the DHCP snooping functionality. To prevent this interference, enter the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode. This command causes DHCP snooping entries to be replicated in the DACLs.

Examples

This example shows how to configure compatibility between webauth and IPSG:

```
Router(config)# mls acl tcam override dynamic dhcp-snooping
```

Related Commands

Command	Description
ip admission	Configures web-based authentication on the interface.
ip dhcp snooping	Enables DHCP snooping.
ip verify source	Enables IP Source Guard on the port.

mls acl tcam share-global

To enable sharing of the global default ACLs, use the **mls acl tcam share-global** command in global configuration mode. To turn off sharing of the global defaults, use the **no** form of this command.

mls acl tcam share-global

no mls acl tcam share-global

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you power cycle one of the DFCs, we recommend that you reset all the DFCs across the ACLs of the different DFCs.

Examples

This example shows how to enable sharing of the global default ACLs:

```
Router(config)# mls acl tcam share-global
```

mls acl vacl apply-self

To enable VACL lookups on software-switched and router-generated packets on the Catalyst 6500 Supervisor Engine 2, use the **mls acl vacl apply-self**command in global configuration mode. To disable VACL lookups for software packets, use the **no** form of this command.

mls acl vacl apply-self

no mls acl vacl apply-self

Syntax Description

This command has no keywords or arguments.

Command Default

VACL lookup on the egress VLAN for software packets are not enabled on switches with Supervisor Engine 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2SXF15	Support for this command was introduced on the Supervisor Engine 2.

Usage Guidelines

On the Supervisor Engine 2 based switches running Cisco IOS Release 12.2(18)SXF15 or a later release, you can enable VACL lookups on software-switched and router generated packets for the VLAN filter configured on the egress VLAN by entering the **mls acl vacl apply-self** command.

On both the Supervisor Engine 720 and Supervisor Engine 32, software-switched packets and router-generated packets are always subjected to VACL lookups on the egress VLAN.

Examples

This example shows how to enable VACL lookups on software-switched and router-generated packets:

```
Router(config)# mls acl vacl apply-self
Router(config)#
```

mls aclmerge algorithm

To select the type of ACL merge method to use, use the **mls aclmerge algorithm**command in global configuration mode.

mls aclmerge algorithm {**bdd**| **odm**}

Syntax Description

bdd	Specifies the binary decision diagram (BDD)-based algorithm.
odm	Specifies the order dependent merge (ODM)-based algorithm.

Command Default

bdd

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The BDD-based ACL merge uses Boolean functions to condense entries into a single merged list of Ternary Content Addressable Memory (TCAM) entries that can be programmed into the TCAM.

You cannot disable the ODM-based ACL merge on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The ODM-based ACL merge uses an order-dependent merge algorithm to process entries that can be programmed into the TCAM.

Note The ODM-based ACL merge supports both security ACLs and ACLs that are used for QoS filtering.

If you change the algorithm method, the change is not retroactive. For example, ACLs that have had the merge applied are not affected. The merge change applies to future merges only.

Use the **show fm summary** command to see the status of the current merge method.

Examples

This example shows how to select the BDD-based ACL to process ACLs:

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)
```

This example shows how to select the ODM-based ACL merge to process ACLs:

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
```

Related Commands

Command	Description
show fm summary	Displays a summary of feature manager information.

mls ip acl port expand

To enable ACL-specific features for Layer 4, use the **mls ip acl port expand** comman d in global configuration mode. To disable the ACL-specific Layer 4 features, use the **no** form of this command.

mls ip acl port expand

no mls ip acl port expand

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 720 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to enable the expansion of ACL logical operations on Layer 4 ports:

```
Router(config)#
mls ip acl port expand
```

mls ip inspect

To permit traffic through any ACLs that would deny the traffic through other interfaces from the global configuration command mode, use the **mls ip inspect** command. Use the **no** form of this command to return to the default settings.

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

Syntax Description

acl-name	ACL name.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

On a Cisco 7600 series routers, when interfaces are configured to deny traffic, the CBAC permits traffic to flow bidirectionally only through the interface that is configured with the **ip inspect** command.

Examples

This example shows how to permit the traffic through a specific ACL (named den-ftp-c):

```
Router(config)# mls ip inspect deny-ftp-c
Router(config)#
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.

mls rate-limit all

To enable and set the rate limiters common to unicast and multicast packets in the global configuration command mode, use the **mls rate-limit all**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit all {**mtu-failure**| **ttl-failure**} *pps* [*packets-in-burst*]

no mls rate-limit all {**mtu-failure**| **ttl-failure**}

Syntax Description

all	Specifies rate limiting for unicast and multicast packets.
mtu-failure	Enables and sets the rate limiters for MTU-failed packets.
ttl-failure	Enables and sets the rate limiters for TTL-failed packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* is **10**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Rate limiters can rate-limit packets that are punted from the data path in the hardware up to the data path in the software. Rate limiters protect the control path in the software from congestion by dropping the traffic that exceeds the configured rate.

Note For Cisco 7600 series routers configured with a PFC3A, enabling the Layer 2 rate limiters has a negative impact on the multicast traffic. This negative impact does not apply to Cisco 7600 series routers configured with a PFC3BXL.

Examples

This example shows how to set the TTL-failure limiter for unicast and multicast packets:

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit layer2

To enable and rate limit the control packets in Layer 2, use the **mls rate-limit layer2** command in global configuration mode. To disable the rate limiter in the hardware, use the **no** form of this command.

mls rate-limit layer2 {**ip-admission**| **l2pt**| **pdu**| **port-security**| **unknown**} *pps* [*packets-in-burst*]

no mls rate-limit layer2 [**l2pt**| **pdu**| **port-security**| **unknown**]

Syntax Description

ip-admission *pps*	Specifies the rate limit for IP admission on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
l2pt *pps*	Specifies the rate limit for control packets in Layer 2 with a protocol-tunneling multicast-MAC address in Layer 2; valid values are from 10 to 1000000 packets per second.
pdu *pps*	Specifies the rate limit for Bridge Protocol Data Unit (BPDU), Cisco Discovery Protocol (CDP), Protocol Data Unit (PDU), and VLAN Trunk Protocol (VTP) PDU Layer 2 control packets; valid values are from 10 to 1000000 packets per second.
port-security *pps*	Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
unknown	Specifies the rate limit for unknown unicast flooding on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* value is 10 and *pps* value has no default setting.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Release	Modification
12.2(18)SXF5	This **port-security** keyword was added.
12.2(33)SXH	The **ip-admission** keyword was added.

Usage Guidelines

MLS provides high-performance hardware-based Layer 3 switching at Layer 2.

This command is not supported on Catalyst 6500 series switches and Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **unknown** keyword is only available on PFC3C line cards. When PFC3C and PFC3B linecards are powered on in the same chassis the chassis will downgrade to the PFC3B linecard and the **unknown** keyword will be unavailable.

You cannot configure the Layer 2 rate limiters if the global switching mode is set to truncated mode.

The following restrictions are pertinent to the use of the **port-security** *pps* keywords and argument:

- The PFC2 does not support the port-security rate limiter.
- The truncated switching mode does not support the port-security rate limiter.
- The lower the value, the more the CPU is protected.

Rate limiters control packets as follows:

- The frames are classified as Layer 2 control frames by the destination MAC address. The destination MAC address used are as follows:
  - 0180.C200.0000 for IEEE BPDU
  - 0100.0CCC.CCCC for CDP
  - 0100.0CCC.CCCD for Per VLAN Spanning Tree (PVST)/Shared Spanning Tree Protocol (SSTP) BPDU
- The software allocates an Local Target Logic (LTL) index for the frames.
- The LTL index is submitted to the forwarding engine for aggregate rate limiting of all the associated frames.

The Layer 2 control packets are as follows:

- General Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)
- BPDUs
- CDP/Dynamic Trunking Protocol (DTP)/Port Aggregation Protocol (PAgP)/UniDirectional Link Detection Protocol (UDLD)/Link Aggregation Control Protocol (LACP) /VTP PDUs
- PVST/SSTP PDUs

If the rate of the traffic exceeds the configured rate limit, the excess packets are dropped at the hardware.

The **pdu** and **l2pt** rate limiters use specific hardware rate-limiter numbers only, such as 9 through 12. Enter the **show mls rate-limit usage** command to display the available rate-limiter numbers. The available numbers

are displayed as “Free” in the output field. If all four of those rate limiters are in use by other features, a system message is displayed telling you to turn off a feature to rate limit the control packets in Layer 2.

When a MAC move occurs and a packet is seen on two ports, the packet is redirected to the software. If one of those ports has the violation mode set to restrict or protect, the packet is dropped in software. You can use the port-security rate limiter to throttle the number of such packets redirected to software. This helps in protecting the software from high traffic rates.

Examples

This example shows how to enable and set the rate limiters for the protocol-tunneling packets in Layer 2:

```
Router(config)# mls rate-limit layer2 l2pt 3000
```

This example shows how to configure the **port-security** rate limiter:

```
Router(config)# mls rate-limit layer2 port-security 500
```

This example shows how to configure the **ip-admission** rate limiter:

```
Router(config)# mls rate-limit layer2 ip-admission 560
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast l3-features

To enable and set the Layer 3 security rate limiters for the unicast packets in the global configuration command mode, use the **mls rate-limit unicast l3-features**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

no mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to set the Layer 3 security rate limiters for the unicast packets:

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv4

To enable and set the rate limiters for the IPv4 multicast packets in the global configuration command mode, use the **mls rate-limit multicast ipv4**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit multicast ipv4 {**connected**| **fib-miss**| **igmp**| **ip-option**| **partial**| **pim**| **non-rpf**} *pps* [*packets-in-burst*]

no mls rate-limit multicast ipv4 {**connected**| **fib-miss**| **igmp**| **ip-option**| **partial**| **pim**| **non-rpf**}

Syntax Description

connected	Enables and sets the rate limiters for multicast packets from directly connected sources.
fib-miss	Enables and sets the rate limiters for the FIB-missed multicast packets.
igmp	Enables and sets the rate limiters for the IGMP packets.
ip-option	Enables and sets the rate limiters for the multicast packets with IP options.
partial	Enables and sets the rate limiters for the multicast packets during a partial SC state.
pim	Enables and sets the rate limiters for the PIM IPv4 multicast packets.
non-rpf	Enables and sets the rate limiters for the multicast packets failing the RPF check.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **100** is programmed for multicast cases.
- **fib-miss** --Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.
- **ip-option** --Disabled.
- **partial** --Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.

Command Modes Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **igmp** and **ip-option**keywords.
12.2(18)SXD	This command was changed to include the **ipv4** keyword.
12.2(33)SXH	This command was changed to add the **pim** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You cannot configure the IPv4 rate limiters if the global switching mode is set to truncated mode.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

The **ip-option** keyword is supported in PFC3BXL or PFC3B mode only.

Examples This example shows how to set the rate limiters for the multicast packets failing the RPF check :

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

This example shows how to set the rate limiters for the multicast packets during a partial SC state:

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

This example shows how to set the rate limiters for the FIB-missed multicast packets:

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6**command in global configuration mode. To disable the rate limiters, use the **no** form of this command.

mls rate-limit multicast ipv6 {**connected pps [packets-in-burst]**| **rate-limiter-name share** {**auto**| **target-rate-limiter**}}

no mls rate-limit multicast ipv6 {**connected**| *rate-limiter-name*}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source ; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
rate-limiter-name	Rate-limiter name; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the “Usage Guidelines” section for additional information.
share	Specifies the sharing policy for IPv6 rate limiters; see the “Usage Guidelines” section for additional information.
auto	Decides the sharing policy automatically.
target-rate-limiter	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the “Usage Guidelines” section for additional information.

Command Default

If the *burst* is not set, a default of **100** is programmed for multicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *rate-limiter-name*argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter*argument must be a rate limiter that is programmed in the hardware and must be the first rate limiterprogrammed for its group.

The table below lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 2: IPv6 Rate Limiters

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class--Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- Static sharing of a rate limiter with another preconfigured rate limiter--When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-cntl** rate limiter with the **default-drop** target rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters--If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast acl

To enable and set the ACL-bridged rate limiters in global configuration command mode, use the **mls rate-limit unicast acl**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast acl {**input**| **output**| **vacl-log**} *pps* [*packets-in-burst*]

Syntax Description

input	Specifies the rate limiters for the input ACL-bridged unicast packets.
output	Specifies the rate limiters for the output ACL-bridged unicast packets.
vacl-log	Specifies the rate limiters for the VACL log cases.
pps	Packets per second; see the “Usage Guidelines” section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **input** --Disabled.
- **output** --Disabled.
- **vacl-log** --Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **mls rate-limit unicast** command was reformatted.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **input** and **output** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases--10 to 1000000 *pps*
- VACL log cases--10 to 5000 *pps*

You cannot change the **vacl-log** *packets-in-burst*keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the i ngress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast acl input 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast cef

To enable and set the Cisco Express Forwarding rate limiters in global configuration command mode, use the **mls rate-limit unicast cef**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast cef {**receive**| **glean**} *pps* [*packets-in-burst*]

Syntax Description

receive	Enables and sets the rate limiters for receive packets.
glean	Enables and sets the rate limiters for ARP-resolution packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **receive** --Disabled.
- **glean** --Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. The default for **glean** was changed to disabled.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

If you enable the CEF rate limiters, the following behaviors occur (if the behavior that is listed is unacceptable, disable the CEF rate limiters):

- If a packet hits a glean/receive adjacency, the packet may be dropped instead of being sent to the software if there is an output ACL on the input VLAN and the matched entry result is deny.

- If the matched ACL entry result is bridge, the packet is subject to egress ACL bridge rate limiting (if turned ON) instead of glean/receive rate limiting.
- The glean/receive adjacency rate limiting is applied only if the output ACL lookup result is permit or there is no output ACLs on the input VLAN.

Examples

This example shows how to set the CEF-glean limiter for the unicast packets:

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast ip

To enable and set the rate limiters for the unicast packets in global configuration command mode, use the **mls rate-limit unicast ip**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast ip {**errors**| **features**| **options**| **rpf-failure**} *pps* [*packets-in-burst*]

mls rate-limit unicast ip icmp {**redirect**| **unreachable acl-drop** *pps*| **no-route** *pps*} [*packets-in-burst*]

no mls rate-limit unicast ip {**errors**| **features**| **icmp** {**redirect**| **unreachable** {**acl-drop**| **no-route**}}| **options**| **rpf-failure**} *pps* [*packets-in-burst*]

Syntax Description

errors	Specifies rate limiting for unicast packets with IP checksum and length errors.
features	Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).
options	Specifies rate limiting for unicast IPv4 packets with options.
rpf-failure	Specifies rate limiting for unicast packets with RPF failures.
pps	Packets per second; see the “Usage Guidelines” section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
icmp redirect	Specifies rate limiting for unicast packets requiring ICMP redirect.
icmp unreachable acl-drop *pps*	Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.
icmp unreachable no-route *pps*	Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.

Command Default

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **10** is programmed as the burst for unicast cases.
- **errors** -- Enabled at **500** *pps* and *packets-in-burst* set to **10**.
- **rpf-failure** --Enabled at **500** *pps* and *packets-in-burst* set to **10**

- **icmp unreachable acl-drop** -- Enabled at **500** *pps* and *packets-in-burst* set to **10**
- **icmp unreachable no-route** -- Enabled at **500** *pps* and *packets-in-burst* set to **10**
- **icmp redirect** -- Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **mls rate-limit unicast** command added the **ip** keyword to the following: • **options** • **icmp** • **rpf-failure** • **errors** • **features** These keywords were changed as follows: • The **features** keyword replaced the **l3-features**keyword. • The **mls rate-limit unicast icmp redirect** command replaced the **mls rate-limit unicast icmp-redirect**command. • The **mls rate-limit unicast icmp unreachable** command replaced the **mls rate-limit unicast icmp-unreachable**command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

To provide OAL support for denied packets, enter the **mls rate-limit unicast ip icmp unreachable acl-drop 0** command.

OAL and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured, use SPAN to capture traffic.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

Note When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

When setting the *pps*, the valid values are **0** and from 10 to 1000000. Setting the *pps* to **0** globally disables the redirection of the packets to the route processor. The **0** value is supported for these rate limiters:

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
- IP rpf failure

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the i ngress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast vacl-log

To enable and set the VACL-log case rate limiters in the global configuration command mode, use the **mls rate-limit unicast vacl-log**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast vacl-log *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases--10 to 1000000 *pps*
- VACL log cases--10 to 5000 *pps*

Setting the *pps* to **0** globally disables the redirection of the packets to the route processor.

You cannot change the **vacl-log** *packets-in-burst*keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the i ngress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the VACL-log case packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode [**tunnel**| **transport**]

no mode

Syntax Description

tunnel >| **transport**	(Optional) Specifies the mode for a transform set: either tunnel or transport mode. If neither **tunnel** nor **transport** is specified, the default (tunnel mode) is assigned.

Command Default

Tunnel mode

Command Modes

Crypto transform configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to change the mode specified for the transform. This setting is only used when the traffic to be protected has the same IP addresses as the IPSec peers (this traffic can be encapsulated either in tunnel or transport mode). This setting is ignored for all other traffic (all other traffic is encapsulated in tunnel mode).

If the traffic to be protected has the same IP address as the IP Security peers and transport mode is specified, during negotiation the router will request transport mode but will accept either transport or tunnel mode. If tunnel mode is specified, the router will request tunnel mode and will accept only tunnel mode.

After you define a transform set, you are put into the crypto transform configuration mode. While in this mode you can change the mode to either tunnel or transport. This change applies only to the transform set just defined.

If you do not change the mode when you first define the transform set, but later decide you want to change the mode for the transform set, you must re-enter the transform set (specifying the transform name and all its transforms) and then change the mode.

If you use this command to change the mode, the change will only affect the negotiation of subsequent IPSec security associations via crypto map entries which specify this transform set. (If you want the new settings to take effect sooner, you can clear all or part of the security association database. See the **clear crypto sa** command for more details.

Tunnel Mode

With tunnel mode, the entire original IP packet is protected (encrypted, authenticated, or both) and is encapsulated by the IPSec headers and trailers (an Encapsulation Security Protocol header and trailer, an Authentication Header, or both). Then a new IP header is prefixed to the packet, specifying the IPSec endpoints as the source and destination.

Tunnel mode can be used with any IP traffic. Tunnel mode must be used if IPSec is protecting traffic from hosts behind the IPSec peers. For example, tunnel mode is used with Virtual Private Networks (VPNs) where hosts on one protected network send packets to hosts on a different protected network via a pair of IPSec peers. With VPNs, the IPSec peers "tunnel" the protected traffic between the peers while the hosts on their protected networks are the session endpoints.

Transport Mode

With transport mode, only the payload (data) of the original IP packet is protected (encrypted, authenticated, or both). The payload is encapsulated by the IPSec headers and trailers (an ESP header and trailer, an AH header, or both). The original IP headers remain intact and are not protected by IPSec.

Use transport mode only when the IP traffic to be protected has IPSec peers as both the source and destination. For example, you could use transport mode to protect router management traffic. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set newer esp-des esp-sha-hmac
 mode transport
 exit
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set--an acceptable combination of security protocols and algorithms.

mode ra

To place the public key infrastructure (PKI) server into Registration Authority (RA) certificate server mode, use the **mode ra**command in certificate server configuration mode. To remove the PKI server from RA certificate mode, use the **no** form of this command.

mode ra [transparent]

no mode ra [transparent]

Syntax Description

transparent	Allows the CA server in RA mode to interoperate with more than one type of CA server.

Command Default

The PKI server is not placed into RA certificate server mode.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(7)T	This command was introduced.
15.1(2)T	This command was modified. In Cisco IOS Release 15.1(2)T, the **transparent** keyword was introduced that allows the IOS CA server in RA mode to interoperate with more than one type of CA server.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS issuing certification authority (CA). If the **mode ra** command is not configured and the certificate server is enabled for the first time, a self-signed CA certificate will be generated and the certificate server will operate as a root CA.

The Cisco IOS certificate server can act as an RA for a Cisco IOS CA or another third party CA. The **transparent** keyword is used if a third-party CA is used.

When the **transparent** keyword is used, the original PKCS#10 enrollment message is not re-signed and is forwarded unchanged. This enrollment message makes the IOS RA certificate server work with CA servers like the Microsoft CA server.

Examples

The following configuration example shows that a RA mode certificate server named "myra" has been configured:

```
Router (config)# crypto pki trustpoint myra
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=cisco, c=us
Router (ca-trustpoint)# exit
Router (config)# crypto pki server myra
Router (cs-server)# mode ra
Router (cs-server)# no shutdown
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.

Command	Description
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

mode secure

To enable the secure mode in the Lightweight Directory Access Protocol (LDAP) server, use the **mode secure**command in LDAP server configuration mode. To disable the secure mode in LDAP server, use the **no** form of this command.

mode secure [no-negotiation]

no mode secure [no-negotiation]

Syntax Description

no-negotiation	(Optional) Specifies the Transport Layer Security (TLS) specific parameter.

Command Default

The secure mode is disabled.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **mode secure** command to establish a TLS connection with the LDAP server. This command will help to secure all the transactions.

Examples

The following example shows how to configure the secure mode on the LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# mode secure no-negotiation
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

mode sub-cs

To place the public key infrastructure (PKI) server into sub-certificate server mode, use the **mode sub-cs**command in certificate server mode. To remove the PKI server from sub-certificate mode, use the **no** form of this command.

mode sub-cs

no mode sub-cs

Syntax Description

This command has no arguments or keywords.

Command Default

The PKI server is not placed into sub-certificate server mode.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS root certification authority (CA). If the **mode sub-cs** command is not configured and the certificate server is enabled for the first time, a self-signed CA certification is generated and the certificate server will operate as a root CA.

Note The **no mode sub-cs** command has no effect if the server has been configured already. For example, if you want to make the subordinate CA a root CA, you must delete the server and re-create it.

Examples

The following configuration example shows that a subordinate certificate server named “sub” has been configured:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# exit
Router (config)# crypto pki server sub
Router (cs-server)# issuer-name CN=sub CA, O=Cisco, C=us
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.

Command	Description
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

monitor event-trace dmvpn

To monitor and control Dynamic Multipoint VPN (DMVPN) traces, use the **monitor event-trace dmvpn** command in privileged EXEC or global configuration mode.

Privileged EXEC

monitor event-trace dmvpn {**dump [merged] pretty**| **nhrp** {**error**| **event**| **exception**}| **clear**| **continuous [cancel]**| **disable**| **enable**| **one-shot**| **tunnel**}

Global Configuration

monitor event-trace dmvpn {**dump-file** *url*| {**nhrp** {**error**| **event**| **exception**}| **tunnel**} {**disable**| **dump-file** *url*| **enable**| **size**| **stacktrace** *value*}}

no monitor event-trace dmvpn {**dump-file** *url*| {**nhrp** {**error**| **event**| **exception**}| **tunnel**} {**disable**| **dump-file** *url*| **enable**| **size**| **stacktrace** *value*}}

Syntax Description

dump	Displays all event traces.
merged	(Optional) Displays entries in all the event traces sorted by time.
pretty	Displays the event traces in ASCII format.
nhrp	Monitors Next Hop Resolution Protocol (NHRP) traces.
error	Monitors NHRP error traces.
event	Monitors NHRP event traces.
exception	Monitors NHRP exception errors.
tunnel	Monitors all tunnel events.
clear	Clears the trace.
continuous	Displays the latest event trace entries continuously.
cancel	(Optional) Cancels continuous display of the latest trace entries.
disable	Disables NHRP or tunnel tracing.
enable	Enables NHRP or tunnel tracing.
one-shot	Clears the trace, sets the running configuration, and then disables the configuration at the wrap point.

tunnel	Monitors all tunnel events.
dump-file *url*	Sets the name of the dump file.
stacktrace *value*	Specifies the trace buffer stack to be cleared first. The stack range is from 1 to 16.

Command Default DMVPN event tracing is disabled.

Command Modes Privileged EXEC (#) Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines You can use the **monitor event-trace dmvpn**command to configure the DMVPN Event Tracing feature. The DMVPN Event Tracing feature provides a trace facility for troubleshooting Cisco IOS DMVPN. This feature enables you to monitor DMVPN events, errors, and exceptions. During runtime, the event trace mechanism logs trace information in a buffer space. A display mechanism extracts and decodes the debug data.

Note You can configure the DMVPN Event Tracing feature in privileged EXEC mode or global configuration mode based on the desired parameters.

Examples The following example shows how to configure a router to monitor and control NHRP event traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp event enable
```

The following example shows how to configure a router to monitor and control NHRP exception traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp exception enable
```

The following example shows how to configure a router to monitor and control NHRP error traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp error enable
```

The following example shows how to configure a router to monitor and control NHRP event traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp event enable
```

The following example shows how to configure a router to monitor and control NHRP exception traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp exception enable
```

The following example shows how to configure a router to monitor and control NHRP error traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp error enable
```

Related Commands

Command	Description
show monitor event-trace dmvpn	Displays DMVPN trace information.

monitor event-trace gdoi

To configure event tracing for the Group Domain of Interpretation (GDOI) software subsystem component, use the **monitor event-trace gdoi** command in global configuration mode.

monitor event-trace gdoi dump-file *url*

monitor event-trace gdoi {**coop**| **exit**| **infra**| **registration**| **rekey**} [**dump-file** *url*| **size** *number-of-entries*| **stacktrace** [*depth*]]

no monitor event-trace gdoi dump-file *url*

no monitor event-trace gdoi {**coop**| **exit**| **infra**| **registration**| **rekey**} [**dump-file** *url*| **size**]

Syntax Description

dump-file	Dump merged traces to a file.
url	Destination to store merged traces.
coop	Monitor cooperative key server (KS) traces.
exit	Monitor GDOI exit traces.
infra	Monitor GDOI infrastructure event traces.
registration	Monitor GDOI registration event traces.
rekey	Monitor GDOI rekey exception errors.
size	Size of the trace.
number-of-entries	Number from 1 to 1000000 that sets the size of the trace.
stacktrace	Trace the call stack at tracepoints (clear the trace buffer first).
depth	Number from 1 to 16 that sets the depth of the stack trace.

Command Default

GDOI event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **monitor event-trace gdoi** command to enable or disable event tracing for GDOI and to configure event trace parameters for the Cisco IOS software GDOI subsystem component.

Note Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative.

Additionally, default settings do not appear in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace** *component* **enable** command will not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace gdoi** command for each instance of a trace.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace gdoi** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for GDOI subsystem component in Cisco IOS software and configure the size to 4096 messages. The trace messages file is set to gdoi-dump in slot0 (flash memory).

```
Device> enable
Device# configure terminal
Device(config)# monitor event-trace gdoi dump-file slot0:gdoi-dump
Device(config)# monitor event-trace gdoi size 4096
```

Related Commands

Command	Description
show monitor event-trace gdoi	Displays event trace messages for the Cisco IOS software GDOI subsystem component.
monitor event-trace gdoi (privileged EXEC)	Configures event tracing for the GDOI software subsystem component.

monitor event-trace gdoi (privileged EXEC)

To configure event tracing for the Group Domain of Interpretation (GDOI) software subsystem component, use the **monitor event-trace gdoi** command in privileged exec mode.

monitor event-trace gdoi dump [**[merged] pretty**]

monitor event-trace gdoi {**coop**| **exit**| **infra**| **registration**| **rekey**} {**clear**| **continuous [cancel]**| **disable**| **dump** [**[merged] pretty**]| **enable**| **one-shot**}

Syntax Description

dump	Dump all event traces.
merged	Dump entries in all event traces sorted by time.
pretty	Dump in ASCII format.
coop	Monitor cooperative key server (KS) traces.
exit	Monitor GDOI exit traces.
infra	Monitor GDOI infrastructure event traces.
registration	Monitor GDOI registration event traces.
rekey	Monitor GDOI rekey exception errors.
clear	Clear the trace.
continuous	Continuously display latest event trace entries.
cancel	Cancel continuous display of latest trace entries.
disable	Disable tracing.
enable	Enable tracing.
one-shot	Clear the trace, set running, then disable at wrap point. Each buffer is a circular linked list that is overwritten when the buffer is full replacing the oldest entry first; this keyword disables overwriting the buffer by filling it once and stopping collection of the event and exit traces when the buffer is full.

Command Default

GDOI event tracing is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **monitor event-trace gdoi** command to enable or disable event tracing for GDOI and to configure event trace parameters for the Cisco IOS software GDOI subsystem component.

Note Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative.

Additionally, default settings do not appear in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace** *component* **enable** command will not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace gdoi** command to display trace messages.

Examples

The following example shows how to disable event tracing for cooperative KSs.

```
Device> enable
Device# monitor event-trace gdoi coop disable
```

Related Commands

Command	Description
show monitor event-trace gdoi	Displays event trace messages for the Cisco IOS software GDOI subsystem component.
monitor event-trace gdoi	Configures event tracing for the GDOI software subsystem component.

monitor event-trace ipv6 spd

To monitor Selective Packet Discard (SPD) state transition events, use the monitor event-trace ipv6 spd command in privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor event-trace ipv6 spd

no monitor event-trace ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **monitor event-trace ipv6 spd** command to check SPD state transition events.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The table below lists default MTU values according to media type.

Table 3: Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if) Connect configuration (xconnect-conn-config) xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support the connect configuration mode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	This command was modified. Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command supports xconnect subinterface configuration mode.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in template configuration mode.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing the MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed: RSP-3-Restart:cbus complex .

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes. The MTU values can be configured to any range that is supported by the corresponding main interface.

MTU Size for an IPSec Configuration

In an IPSec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, then the MTU value is automatically overwritten and given a value of 256 bytes.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490 bytes). A client is configured with the range supported by the corresponding main interface. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

VRF-Aware Service Infrastructure Interfaces

The mtu command does not support the VRF-Aware Service Infrastructure (VASI) type interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, the following valid values are applicable:

- For the SVI ports: from 64 to 9216 bytes
- For the GE-WAN+ ports: from 1500 to 9170 bytes
- For all other ports: from 1500 to 9216 bytes

You can receive jumbo frames on access subinterfaces also. The MTU values can be configured to any range that is supported by the corresponding main interface. If you enable the jumbo frames, the default is 64 bytes for the SVI ports and 9216 bytes for all other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

While configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following overhead:
  - Layer 2 header--14 bytes
  - Dot1Q header--4 bytes
  - CRC--4 bytes
- If you are using MPLS, be sure that the **mpls mtu** command is configured with a value less than or equal to the interface MTU.
- If you are using MPLS labels, you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Device(config)# interface serial 1
Device(config-if)# mtu 1000
```

Examples

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Device(config)# interface GigabitEthernet3/0/0
Device(config-if)# mtu 1800
```

Examples

The following example shows how to specify an MTU size on a pseudowire interface:

```
Device(config)#  interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

Examples

The following example shows how to configure a template and specify an MTU size in template configuration mode: :

```
Device(config)#  template type pseudowire template1
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

name

To configure the redundancy group with a name, use the **name**command in redundancy application group configuration mode. To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*

no name *group-name*

Syntax Description

group-name	Name of the redundancy group.

Command Default

The redundancy group is not configured with a name.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

name (view)

To change the name of a lawful intercept view, use the **name**command in view configuration mode. To return to the default lawful intercept view name, which is "li-view," use the **no** form of this command.

name *new-name*

no name *new-name*

Syntax Description

new-name	Lawful intercept view name.

Command Default

A lawful intercept view is called "li-view."

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Only a system administrator or a level 15 privilege user can change the name of a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view and change the view name to "myliview":

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# name myliview
Router(config-view)# end
```

Related Commands

Command	Description
li-view	Initializes a lawful intercept view.

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

named-key

To specify which peer's RSA public key you will manually configure and enter public key configuration mode, use the **named-key** command in public key chain configuration mode. This command should be used only when the router has a single interface that processes IP Security (IPSec).

named-key *key-name* [**encryption**| **signature**]

Syntax Description

key-name	Specifies the name of the remote peer's RSA keys. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special-usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special-usage key.

Command Default

If neither the **encryption** nor the **signature** keyword is used, general-purpose keys will be specified.

Command Modes

Public key chain configuration.

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command or the **addressed-key** command to specify which IPSec peer's RSA public key you will manually configure next.

Follow this command with the **key-string** command to specify the key.

If you use the **named-key** command, you also need to use the **address** public key configuration command to specify the IP address of the peer.

If the IPSec remote peer generated general purpose RSA keys, do not use the **encryption** or **signature** keyword.

If the IPSec remote peer generated special usage keys, you must manually specify both keys: perform this command and the **key-string** command twice and use the **encryption** and **signature** keywords in turn.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-purpose keys.

```
crypto key pubkey-chain rsa
  named-key otherpeer.example.com
  address 10.5.5.1
  key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4
 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
 D58AD221 B583D7A4 71020301 0001
 quit
 exit
  addressed-key 10.1.1.2 encryption
  key-string
 00302017 4A7D385B 1234EF29 335FC973
 2DD50A37 C4F4B0FD 9DADE748 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8
 08407685 2F2190A0 0B43F1BD 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B
 90288A26 DBC64468 7789F76E EE21
 quit
  exit
  addressed-key 10.1.1.2 signature
  key-string
 0738BC7A 2BC3E9F0 679B00FE 098533AB
 01030201 42DD06AF E228D24C 458AD228
 58BB5DDD F4836401 2A2D7163 219F882E
 64CE69D4 B583748A 241BED0F 6E7F2F16
 0DE0986E DF02031F 4B0B0912 F68200C4
 C625C389 0BFF3321 A2598935 C1B1
 quit
  exit
  exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

nas

To add an access point or router to the list of devices that use the local authentication server, use the **nas**command in local RADIUS server configuration mode. To remove the identity of the network access server (NAS) that is configured on the local RADIUS server, use the **no** form of this command.

nas *ip-address* **key shared-key**

no nas *ip-address* **key shared-key**

Syntax Description

ip-address	IP address of the access point or router.
key	Specifies a key.
shared-key	Shared key that is used to authenticate communication between the local authentication server and the access points and routers that use this authenticator.

Command Default

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following command adds the access point having the IP address 192.168.12.17 to the list of devices that use the local authentication server, using the shared key named shared256.

```
Router(config-radsrv)# nas 192.168.12.17 key shared256
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.

Command	Description
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

nasi authentication

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

nasi authentication {**default**| *list-name*}

no nasi authentication {**default**| *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication nasi** command.
list-name	Uses the list created with the **aaa authentication nasi**command.

Command Default

Uses the default set with the **aaa authentication nasi** command.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is not specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.

Caution If you use a *list-name* value that was not configured with the **aaa authentication nasi**command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4
 nasi authentication default
```

The following example specifies that the AAA authentication list called *list1*be used on line 7:

```
line 7
 nasi authentication list1
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

nat (IKEv2 profile)

To configure Network Address Translation (NAT) keepalive for Internet Key Exchange Version 2 (IKEv2), use the **nat**command in IKEv2 profile configuration mode. To delete NAT keepalive configuration, use the **no** form of this command.

nat keepalive *interval*

no nat keepalive

Syntax Description

keepalive *interval*	Specifies the NAT keepalive interval in seconds.

Command Default

NAT keepalive is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to configure NAT keepalive. NAT keepalive configuration specified in an IKEv2 profile overrides the global configuration. NAT keepalive prevents the NAT translation entries from deletion in the absence of any traffic when there is NAT between IKE peers.

Examples

The following example shows how to specify the NAT keepalive interval:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# nat keepalive 500
```

Related Commands

Command	Description
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 profile	Defines an IKEv2 profile.

nbns-list

To enter the webvpn NBNS list configuration mode to configure a NetBIOS Name Service (NBNS) server list for Common Internet File System (CIFS) name resolution, use the **nbns-list** command in webvpn context configuration mode. To remove the NBNS server list from the SSL VPN context configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list *name*

Syntax Description

name	Name of the NBNS list. The name can be up to 64 characters in length. This argument is case sensitive.

Command Default

Webvpn NBNS list configuration mode is not entered, and a NBNS server list cannot be configured.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The NBNS server list is used to configure a list of Windows Internet Name Service (WINS) to resolve Microsoft file-directory shares. Entering the **nbns-list**command places the router in webvpn NBNS list configuration mode. You can specify up to three NetBIOS name servers. A single server is configured as the master browser if multiple servers are specified in the server list.

Note NBNS and CIFS resolution is supported only on Microsoft Windows 2000 or Linux Samba servers.

Examples

The following example configures an NBNS server list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master

Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5

Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5

Router(config-webvpn-nbnslist)#
```

Related Commands

Command	Description
nbns-server	Adds a server to an NBNS server list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

nbns-list (policy group)

To attach a NetBIOS name service (NBNS) server list to a policy group configuration, use the **nbns-list**command in webvpn group policy configuration mode. To remove the NBNS server list from the policy group configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list

Syntax Description

name	Name of the NBNS server list that was configured in webvpn context configuration mode.

Command Default

An NBNS server list is not attached to a policy group configuration.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

Examples

The following example applies the NBNS server list to the policy group configuration:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master

Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5

Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5

Router(config-webvpn-nbnslist)# exit

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# nbns-list SERVER_LIST

Router(config-webvpn-group)#
```

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
nbns-server	Adds a server to an NBNS server list.
policy group	Enters webvpn group policy configuration mode to configure a group policy.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

nbns-server

To add a server to a NetBIOS name service (NBNS) server list, use the **nbns-server** command in webvpn NBNS list configuration mode. To remove the server entry from the NBNS server list, use the **no** form of this command.

nbns-server *ip-address* **[master]** [**timeout** *seconds*] [**retries** *number*]

no nbns-server *ip-address* **[master]** [**timeout** *seconds*] [**retries** *number*]

Syntax Description

ip-address	The IPv4 address of the NetBIOS server.
master	(Optional) Configures a single NetBIOS server as the master browser.
timeout *seconds*	(Optional) Configures the length of time, in seconds, that the networking device will wait for a query reply before sending a query to another NetBIOS server. A number from 1 through 30 can be configured for this argument.
retries *number*	(Optional) Number of times that the specified NetBIOS server will be queried. A number from 0 through 10 can be configured for this argument. Entering the number 0 configures the networking device not to resend a query.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

timeout 2 **retries** 2

Command Modes

Webvpn NBNS list configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The server specified with the *ip-address*argument can be a primary domain controller (PDC) in a Microsoft network. A Windows Internet Naming Service (WINS) server cannot and should not be specified. When multiple NBNS servers are specified, a single server is configured as master browser.

Examples

The following example adds three servers to an NBNS server list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master

Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5

Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
```

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

netmask

To specify the subnet mask to be used by the client for local connectivity, use the **netmask** command in ISAKMP group configuration mode or IKEv2 group configuration mode. To disable the mask, use the **no** form of this command.

netmask *mask*

no netmask *mask*

Syntax Description

mask	Subnet mask address.

Command Default

Default mask is used.

Command Modes

ISAKMP group configuration (config-isakmp-group) IKEv2 client group configuration (config-ikev2-client-config-group)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Easy VPN remote.

Usage Guidelines

Use this command to specify the subnet mask for the IP address assigned to the client.

Examples

The following example shows that the subnet mask 255.255.255.255 is to be downloaded to the client:

```
crypto isakmp client configuration group group1
 netmask 255.255.255.255
```

no crypto engine software ipsec

To disable hardware crypto engine failover to the software crypto engine, use the **no crypto engine software ipsec**command in global configuration mode. To reenable failover, use the **crypto engine software ipsec**form of this command.

no crypto engine software ipsec

crypto engine software ipsec

Syntax Description

This command has no arguments or keywords.

Command Default

Failover is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1E	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command for those situations in which the amount of IP Security (IPSec) traffic is more than can be handled (because of bandwidth) by the software routines on the CPU.

Examples

The following example shows that hardware crypto engine failover to the software crypto engine has been disabled:

```
no crypto engine software ipsec
```

The following example shows that hardware crypto engine failover has been reenabled:

```
crypto engine software ipsec
```

Related Commands

Command	Description
crypto engine accelerator	Enables the onboard hardware accelerator of the router for IPSec encryption.

no crypto xauth

To ignore extended authentication (Xauth) during an Internet Key Exchange (IKE) Phase 1 negotiation, use the **no crypto xauth** command in global configuration mode. To consider Xauth proposals, use the **crypto xauth** command.

no crypto xauth *interface*

crypto xauth *interface*

Syntax Description

interface	Interface whose IP address is the local endpoint to which the remote peer will send IKE requests.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **no** version of this command was introduced to support Unity clients that do not require Xauth when using Internet Security Association and Key Management Protocol (ISAKMP) profiles.

Note This command does not support loopback interfaces.

Examples

The following example shows that Xauth proposals on Ethernet 1/1 are to be ignored:

```
no crypto xauth Ethernet1/1
```

no ip inspect

To turn off Context-based Access Control (CBAC) completely at a firewall, use the **no ip inspect** command in global configuration mode.

no ip inspect

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Turn off CBAC with the **no ip inspect** global configuration command.

Note The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults. All existing sessions are deleted and their associated access lists are removed.

Examples

The following example turns off CBAC at a firewall:

```
no ip inspect
```

no ip ips sdf builtin

To instruct the router not to load the built-in signatures if it cannot find the specified signature definition files (SDFs), use the **no ip ips sdf builtin**command in global configuration mode.

no ip ips sdf builtin

Syntax Description

This command has no arguments or keywords.

Command Default

If the router fails to load the SDF, the router will load the default, built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelin

Caution If the **no ip ips sdf builtin** command is issued and the router running Intrusion Prevention System (IPS) fails to load the SDF, you will receive an error message stating that IPS is completely disabled.

Examples

The following example shows how to instruct the router not to refer to the default, built-in signature if the attack-drop.sdf file fails to load:

```
Router(config) no ip ips sdf builtin
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router will load the SDF.

non-standard (config-radius-server)

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **non-standard** command in RADIUS server configuration mode. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

non-standard

no non-standard

Syntax Description

This command has no arguments or keywords.

Command Default

Nonstandard RADIUS attributes are not supported.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **non-standard** command to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **non-standard** command in RADIUS server configuration mode.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example shows how to specify a vendor-proprietary RADIUS server host 192.0.2.2:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# non-standard
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

Command	Description
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

object-group (Catalyst 6500 series switches)

To define object groups that you can use to optimize your configuration, use the **object-group** global configuration mode command. To remove object groups from the configuration use the **no** form of this command .

object-group ip {**address** *obj-grp-id*| **port** *obj-grp-id*}

no object-group ip {**address** *obj-grp-id*| **port** *obj-grp-id*}

Syntax Description

ip	Specifies the IP object group.
address *obj-grp-id*	Specifies the IP address of the object group and allows you to define the object group name and enter IP-address object-group configuration mode. See the "Usage Guidelines" section for more information.
port *obj-grp-id*	Specifies the IP port of the object group and allows you to create or modify a PBACL protocol port object group. See the "Usage Guidelines" section for more information.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode	Security Context			
Routed	Transparent	Single	Multiple		
			Context	System	
Global configuration	Yes	Yes	Yes	Yes	No

Command History

Release	Modification
12.2(33)SXH	This command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command supports IPv4 and IPv6 addresses.

Objects such as hosts, protocols, or services can be grouped, and then you can issue a single command using the group name to apply to every item in the group.

When you define a group with the **object-group** command and then use any security appliance command, the command applies to every item in that group. This feature can significantly reduce your configuration size.

Once you define an object group, you must use the **object-group** keyword before the group name in all applicable security appliance commands as follows:

```
Router# show running-config object-group group-name
```
where group-name is the name of the group.

This example shows the use of an object group once it is defined:

```
Router(config)# access-list access_list_name permit tcp any object-group group-name
```
In addition, you can group access list command arguments:

Individual Argument	Object Group Replacement
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp-type	**object-group** *icmp-type*

You can group commands hierarchically; an object group can be a member of another object group.

To use object groups, you must do the following:

- Use the object-group keyword before the object group name in all commands as follows:

```
Router(config)# access-list acl permit tcp object-group remotes object-group locals
object-group eng-svc
```
where **remotes** and **locals** are sample object group names.

- The object group must be nonempty.
- You cannot remove or empty an object group if it is being used in a command.

Use the **exit**, **quit**, or any valid config-mode commands such as **access-list** to close an object-group mode and exit the object-group main command.

The **show running-config object-group** command displays all defined object groups by their grp-id when the **show running-config object-group** *group-id* command is entered, and by their group type when you enter the **show running-config object-group** *group-type* command. When you enter the **show running-config object-group** command without an argument, all defined object groups are shown.

Use the **clear configure object-group** command to remove a group of previously defined object-group commands. Without an argument, the **clear configure object-group** command lets you to remove all defined object groups that are not being used in a command. Use of the group-type argument removes all defined object groups that are not being used in a command for that group type only.

You can use all other security appliance commands in an object-group mode, including the **show running-config** and **clear configure** commands

Commands within the object-group mode appear indented when displayed or saved by the **show running-config object-group**, **write**, or **config** commands.

Commands within the object-group mode have the same command privilege level as the main command.

When you use more than one object group in an access-list command, the elements of all object groups that are used in the command are linked, starting with the elements of the first group with the elements of the second group, then the elements of the first and second groups together with the elements of the third group, and so on.

The starting position of the description text is the character right immediately following the white space (a blank or a tab) following the description keyword.

When you enter the object-group ip address command, the prompt changes to Router(config-ipaddr-ogroup)# and allows you to create or modify a PBACL protocol port object group.

The following IP address object-group configuration commands are available:

- **A.B.C.D** --Specifies the network address of the object-group members.
- **end** --Exits from configuration mode.
- **exit** --Exits from IP object-group configuration mode.
- **host** *address* or **host** *name*--Specifies the host address or name of the object-group member.
- **no** --Negates or sets the default values of a command.

Use the **no** form of the command to delete the object group with the specified name.

When you enter the object-group ip port command, the prompt changes to Router(config-port-ogroup)# and allows you to define the object group name and enter port object-group configuration mode. The following port object-group configuration commands are available:

- **end** --Exits from configuration mode.
- eq number--Matches only packets on a given port number; valid values are from 0 to 65535.
- **exit** --Exits from the IP object-group configuration mode.
- gt number--Matches only packets on a given port number; valid values are from 0 to 65535.
- lt number--Matches only packets with a lower port number; valid values are from 0 to 65535.
- neq number--Matches only packets with a lower port number; valid values are from 0 to 65535.
- **no** --Negates or sets default values of a command.
- range number number--Matches only packets in the range of port numbers; valid values are from 0 to 65535.

Use the **no** form of the command to delete the object group with the specified name.

Examples

This example shows how to create an object group with three hosts and a network address:

```
Router(config)# object-group ip address myAG
Router(config-ipaddr-pgroup)# host 10.20.20.1
```

```
Router(config-ipaddr-pgroup)# host 10.20.20.5
Router(config-ipaddr-pgroup)# 10.30.0.0 255.255.0.0
```

This example shows how to create a port object group that matches protocol port 100 and any port greater than 200, except 300:

```
Router(config)# object-group ip port myPG
Router(config-port-pgroup)# eq 100
Router(config-port-pgroup)# gt 200
Router(config-port-pgroup)# neq 300
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

object-group network

To define network object groups for use in object group-based access control lists (ACLs) and enter network group configuration mode, use the **object-group network** command in global configuration mode. To remove network object groups from the configuration, use the **no** form of this command.

object-group network *object-group-name*

no object-group network *object-group-name*

Syntax Description

object-group-name	Name for a network type of object group. *object-group-name* is a sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods (.). The *object-group-name* must start with a letter.

Command Default

No network object groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.0(1)M	This command was modified. The **any** command was added as a command in network group configuration mode.
Cisco IOS XE Release 3.12S	This command was integrated into Cisco IOS XE Release 3.12S. The **any** and **range** commands in network group configuration mode are not supported.

Usage Guidelines

A network object group is a group of any of the following objects: hostnames, host IP addresses, subnets, ranges of IP addresses, or existing network object groups. A network object group is an ordered list and can be used in an ACL or in other commands. You can use a single command using the group name to apply to every object in the group.

This command supports only IPv4 addresses.

When you configure the **object-group network** command, the command mode changes to network group configuration mode (config-network-group) and allows you to populate or modify a network object-group ACL. The following commands are available in network group configuration mode:

- **any**—Specifies any IP address for an object group. This command allows any IP address in the range of 0.0.0.0 to 255.255.255.255 to be used in an object group.
- **description** *description-text*—Description of the object or object group (you can use up to 200 characters).
- **group-object** *nested-object-group-name*—Specifies an existing network object group (child) to be included in the current object group (parent).
- **host** {*host-address* | *host-name*}—Specifies the host object. You must use an IPv4 address for the host address.
- *network-address* {*/nn* | *network-mask*}—Specifies a subnet object for the object group.
- **range** *host-address1 host-address2*—Species a range of host IP addresses for an object group.

Note In Cisco IOS XE releases, the **any** and **range** commands are not supported.

Commands within network group mode have the same command privileges as the main command. Commands within network group mode appear indented when saved or displayed using the **write memory** or **show running-config** commands.

The type of child object group must match the type of the parent (for example, if you create a network object group, the child object group that you specify must be another network object group). The **object-group network** command supports unlimited number of nested object groups; however, we recommend that you configure a maximum of only two levels.

You can duplicate objects in an object group when the duplication is because these objects are part of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).

When you use the *network-address*/*nn* command to create a subnet object, for example 209.165.201.0 /27, the 27 most significant bits are allocated for the network prefix number, and the remaining 5 bits are reserved for the host address. If the same subnet object is created using the *network-address network-mask* command, the command appears as 209.165.201.31 255.255.255.224. Here, the subnet mask is 255.255.255.224. The default subnet mask is 255.255.255.255.

Using a subnet mask of 0.0.0.0 includes any address in the range from 0.0.0.0 to 255.255.255.255 in the subnet object and using 0.0.0.0 gives the subnet object the same range as the range specified by the **any** command. Using a range from 0.0.0.0 to 255.255.255.255 specifies that any IP address can be used as a host IP address and this configuration is similar to configuring the **any** command, which specifies that any IP address can be used.

If the same IP address is used for host-address1 and host-address2, the effect is the same as using the **host** command; the identical IP address becomes the single host IP address for the object group.

Use the **no** form of the command to delete the object group. You cannot delete an object group that is used within an ACL or a Class-Based Policy Language (CPL) policy.

Examples

The following example shows how to configure a network object group named my-network-object-group that contains two hosts and a subnet as objects.

```
Device> enable
Device# configure terminal
Device(config)# object-group network my-network-object-group
```

```
Device(config-network-group)# host 10.20.20.1
Device(config-network-group)# host 10.20.20.5
Device(config-network-group)# 10.30.0.0 255.255.0.0
```

The following example shows how to configure a network object group named sjc-ftp-servers that contains two hosts , a subnet, and an existing object group (child) named sjc-eng-ftp-servers as objects.

```
Device> enable
Device# configure terminal
Device(config)# object-group network sjc-ftp-servers
Device(config-network-group)# host sjc.eng.ftp
Device(config-network-group)# host 172.23.56.195
Device(config-network-group)# 209.165.200.225 255.255.255.224
Device(config-network-group)# group-object sjc-eng-ftp-servers
```

The following example creates an object group called printer-users and specifies any IP address for the object group:

```
Device> enable
Device# configure terminal
Device(config)# object-group network printer-users
Device(config-network-group)# description sw-engineers
Device(config-network-group)# any
```

The following example creates an object group called research and specifies a range of host IP addresses for the object group:

```
Device> enable
Device# configure terminal
Device(config)# object-group network research
Device(config-network-group)# description engineering-research
Device(config-network-group)# range 209.165.202.129 255.255.255.255
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or object-group ACL that denies packets.
ip access-group	Applies an ACL or object-group ACL to an interface or a service policy map.
ip access-list	Defines an IP access list or object-group ACL by name or number.
object-group service	Defines service object groups for use in object-group ACLs.
permit	Sets conditions in a named IP access list or object-group ACL that permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured.

object-group security

To create an object group to identify traffic coming from a specific user or endpoint, use the **object-group security** command in global configuration mode. To remove the object group, use the **no** form of this command.

object-group security *name*

no object-group security *name*

Syntax Description

name	Object group name.

Command Default

No object group is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

Creating an object group enters object-group identity configuration mode, where a security group can be specified for the object group with a Security Group Tag (SGT) ID. The SGT ID is used by a Security Group Access (SGA) zone-based firewall to apply an enforcement policy by filtering on this SGT ID. The **object-group security** command is used in the class map configuration of the SGA zone-based firewall.

Note A policy map must also be configured for the SGA zone-based firewall.

Examples

The following example shows how the **object-group security** command is used in the class map configuration of the SGA zone-based firewall:

```
Device(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# class-map type inspect xmatch-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# end
```

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
group-object	Specifies a nested reference to a type of user group.
match group-object security	Matches traffic from a user in the security group.
security-group	Specifies the membership of the security group for an object group.
show object-group	Displays the content of all user groups.

object-group service

To define service object groups for use in object-group-based access control lists (ACLs), use the **object-group service** command in global configuration mode. To remove service object groups from the configuration, use the **no** form of this command.

object-group service *object-group-name*

no object-group service *object-group-name*

Syntax Description

object-group-name	Name of a service type of object group.

Command Default

No service object groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.12S	This command was integrated into Cisco IOS XE Release 3.12S.

Usage Guidelines

A service object group is a group of any of the following objects:

- Source and destination protocol ports (such as Telnet or SNMP)
- Internet Control Message Protocol (ICMP) types (such as echo, echo-reply, or host-unreachable)
- Top-level protocols (such as TCP, UDP, or Encapsulating Security Payload [ESP])
- Existing service object groups

A service object group is an ordered list and can be used in an ACL or other commands. You can use a single command using the group name to apply to every object in the group.

This command supports only IPv4 addresses.

Commands within the service group configuration mode appear indented when saved or displayed using the **write memory** or **show running-config** commands.

Commands within the service group configuration mode have the same command privilege level as the main command.

When you use more than one object group in an access-list command, the elements of all object groups that are used in the command are linked, starting with the elements of the first group with the elements of the

second group, then the elements of the first and second groups together with the elements of the third group, and so on.

When you configure the **object-group service** command, configuration mode changes to service group configuration mode (config-service-group) allows you to populate or modify a service-object-group ACL. The following commands are available in service group configuration mode:

- **description** *description-text*—Description of the object or object group (you can use up to 200 characters).
- **group-object** *nested-object-group-name*—Specifies an existing network object group (child) to be included in the current object group (parent).
- **tcp-udp**—Specifies the TCP or UDP protocol.
- *protocol*—Specifies an IP protocol number or name. See the CLI help (?) to view the supported protocols.

The type of child object group must match the type of the parent (for example, if you are create a service object group, the child group you specify must be another service object group).

You can duplicate objects in an object group when the duplication is because these objects are part of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).

The command supports unlimited number of nested object groups; however, we recommend that you configure a maximum of only two levels.

Use the **no** form of the command to delete the object group. You cannot delete an object group that is being used within an ACL or CPL policy.

Examples

This example shows how to create a service object group named service-object-group:

```
Device> enable
Device# configure terminal
Device(config)# object-group service my-service-object-group
Device(config-service-group)# group-object serv-object1
Device(config-service-group)# tcp 200
Device(config-service-group)# ip
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or object-group ACL that denies packets.
ip access-group	Applies an ACL or object-group ACL to an interface or a service policy map.
ip access-list	Defines an IP access list or object-group ACL by name or number.
object-group network	Defines network object groups for use in object-group ACLs.

Command	Description
permit	Sets conditions in a named IP access list or object-group ACL that permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured

occur-at (ips-auto-update)

To define a preset time for which the Cisco IOS Intrusion Prevention System (IPS) automatically obtains updated signature information, use the **occur-at**command in IPS-auto-update configuration mode.

occur-at [**monthly**| **weekly**] *day minutes hours*

Syntax Description

monthly	Monthly update option in days of the month from 1 to 31, minutes from the top of the hour from 0 to 59 and hours of the day from 0 to 23, in which automatic signature updates occur.
weekly	Weekly update option in days of the week from 0 to 6, minutes from the top of the hour from 0 to 59 and hours of the day from 0 to 23, in which automatic signature updates occur.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration (config-ips-auto-update)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T	The command was modified with the **monthly** and **weekly** keywords in Cisco IOS Release 12.4(22)T.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, issue the **occur-at** command to define how often the Cisco IOS IPS signature files should be automatically updated.

Examples

The following example shows how to configure automatic signature updates and set the frequency in which updates are made. In this example, the signature package file is pulled from the TFTP server at the third hour of the 5 day of the month, at the 56th minute of this hour.

Note Adjustments are made for months without 31 days and daylight savings time.

```
Router# clock set ?
hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on console.
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at monthly 5 56 3
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml

Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
minutes (0-59) : 56
hours (0-23) : 3
days of month (1-31) : 5
days of week: (0-6) :
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
cisco	Enables automatic signature updates from Cisco.com.

ocsp

To specify online certificate status protocol (OCSP) settings for the public key infrastructure (PKI) trustpool, use the **ocsp** command in ca-trustpool configuration mode. To disable the OCSP server or return to the default, use the **no** form of this command.

ocsp {**disable-nonce**| **url** *url*}

no ocsp {**disable-nonce**| **url** *url*}

Syntax Description

disable-nonce	Disables the OCSP Nonce Extension.
url *url*	Specifies the OCSP server URL to override (if one exists) in the Authority Info Access (AIA) extension of the certificate. All certificates associated with a configured PKI trustpool are checked by the OCSP server at the specified HTTP URL. The URL can be a hostname, an IPv4 address, or an IPv6 address.

Command Default

The router uses the OCSP server URL in the AIA extension of the certificate. The revocation check fails if no URL exists.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

A central OCSP server is configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers so that devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

If the OCSP URL is specified through the HTTP file system, then the URL must be written in the following formats:

- http://*OCSPname*:80, where *OCSP_name* is the Domain Name System (DNS) of the OCSP server.
- http://*ipv4-address*:80. For example: http://10.10.10.1:80.

- http://*[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL.

Examples

The following example shows how to configure your router to use the OCSP server at the http://ocspts.identrust.com URL:

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# ocsp url http://ocspts.identrust.com
Router(ca-trustpool)# revocation-check ocsp none
```

Note If the server is down, the revocation check is ignored.

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.

Command	Description
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

ocsp url

To specify the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in the Authority Info Access (AIA) extension of the certificate, use the **ocsp url** command in ca-trustpoint configuration mode. To disable the OCSP server, use the **no** form of this command.

ocsp url *url*

no ocsp url *url*

Syntax Description

url	All certificates associated with a configured trustpoint are checked by the OCSP server at the specified HTTP URL. The URL can be a hostname, IPv4 address, or an IPv6 address.

Command Default

The router uses the OCSP server URL in AIA extension of the certificate. If a URL does not exist, then the revocation check fails.

Command Modes

Ca-trustpoint configuration (config-ca-trustpoint)

Command History

Release	Modification
12.3(2)T	This command was introduced.
15.2(1)T	This command was modified. Support for specifying the IPv6 address in a URL for the OCSP server was added.

Usage Guidelines

A central OCSP server is configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers so that devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

The OCSP URL is specified through the HTTP file system, then the URL must be written in the following formats:

- http://*OCSP_name*:80, where *OCSP_name* is the Domain Name System (DNS) of the OCSP server.
- http://*ipv4-address*:80. For example: http://10.10.10.1:80
- *http:///[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL.

Examples

The following example shows how to configure your router to use the OCSP server at the HTTP URL http://myocspserver:81.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

The following example shows how to configure your router to use the OCSP server at the IPv6 HTTP URL http://[2001DB8:1:1::2]:80.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://[2001DB8:1:1::2]:80
Router(ca-trustpoint)# revocation-check ocsp none
```

Note If the server is down, the revocation check is ignored.

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment url (ca-trustpoint)	Specifies the enrollment parameters of a CA.
revocation-check	Checks the revocation status of a certificate.

on

To specify the location where Rivest, Shamir, and Adelman (RSA) keys will be generated upon initial auto enrollment, use the **on** command in ca-trustpoint configuration mode.

on *devicename:*

Syntax Description

devicename:	Specifies the RSA key storage device.

Command Default

Keys are generated and stored in NVRAM.

Command Modes

Ca-trustpoint

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Locations that may be specified include a USB token, local disk, or NVRAM.

A USB token may be used as a cryptographic device in addition to a storage device. Using a USB token as a cryptographic devices allows RSA operations such as key generation, signing, and authentication to be performed on the token. Private keys are not distributed and remain on the token by default, however you may configure the private key storage location.

Keys that reside on a USB token, or on-token keys, are saved to persistent token storage when they are generated. Key deletion will remove the on-token keys from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from non-token storage locations only when the **write memory** or similar command is issued.)

Examples

The following example shows the configuration for the “mytp-A” certificate server and its associated trustpoint, where RSA keys generated by the initial auto enrollment for the trustpoint will be stored on a USB token, “usbtoken0”:

```
crypto pki server mytp-A
   database level complete
   issuer-name CN=company, L=city, C=country
   grant auto
! Specifies that certificate requests will be granted automatically.
!
crypto pki trustpoint mytp-A
   revocation-check none
   rsakeypair myTP-A
   storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:.
   on usbtoken0:
```

```
! Specifies that keys generated on initial auto enroll will be generated on and stored on
! usbtoken0:
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
crypto key import rsa	Imports RSA key pairs.
crypto pki trustpoint	Declares the trustpoint that the router will use.

one-minute

To define the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions, use the **one-minute**command in parameter-map type inspect configuration mode. To disable the value, use the **no** form of this command.

one-minute {**low** *number-of-connections*| **high** *number-of-connections*}

no one-minute {**low** *number-of-connections*| **high** *number-of-connections*}

Syntax Description

low *number-of-connections*	Number of new unestablished sessions that will cause the system to stop deleting half-open sessions.
high *number-of-connections*	Number of new unestablished sessions that will cause the system to start deleting half-open sessions.

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **one-minute**subcommand after you enter the **parameter-map type inspect** command.

Enter the **one-minute** command twice; once to specify a high number at which the system will start deleting half-open sessions, and once to specify a low number at which the system will stop deleting half-open sessions.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example causes the system to start deleting half-open sessions when there are 300 unestablished sessions, and to stop deleting half-open sessions when there are 400 unestablished systems:

```
parameter-map type inspect internet-policy
 one minute high 400
 one minute low 300
```

Related Commands

Command	Description
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

other-config-flag

To verify the advertised “other” configuration parameter, use the **other-config-flag** command in RA guard policy configuration mode.

other-config-flag {**on**| **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

out-of-band telemetry

To enable out-of-band telemetry and Cloud Web Security content-scan exception rules, use the **out-of-band telemetry** command in parameter-map type inspect configuration mode. To disable out-of-band telemetry and Cloud Web Security content-scan exception rules, use the **no** form of this command.

out-of-band telemetry interval *interval*

no out-of-band telemetry interval

Syntax Description

interval *interval*	Specifies the Cloud Web Security content-scan telemetry interval, in minutes. The range is from 5 to 43200.

Command Default

Out-of-band telemetry and Cloud Web Security content-scan exception rules are not enabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Telemetry is an automated communications process in which measurements are made and data that is collected at remote sites is transmitted to receiving equipment for monitoring.

The device on which Cloud Web Security is configured is monitored, and data is generated periodically. Because most of these devices do not have a large amount of memory or secondary storage, the generated data is exported and stored in the Cloud Web Security server. The device connects to a URL hosted by the Cloud Web Security server by using the HTTP POST method to send telemetry data periodically.

Because the Cloud Web Security server does not have information about all web traffic, a connector (a persistent, out-of-band secure channel between the device and the Cloud Web Security server) periodically sends all exception rules to the server. The connector makes a POST request and pushes all exception rules to a URL. This URL is separate from the telemetry URL.

Content scan does a scan of the HTTP and secure HTTP (HTTPS) traffic to protect the Cloud Web Security from malware attacks.

Examples

The following example shows how to enable out-of-band telemetry, which allows the storing of messages generated by the device on which Cloud Web Security is configured:

```
Device# configure terminal
Device(config)# parameter-map type cws
Device(config-profile)# out-of-band telemetry interval 60
Device(config-profile)# end
```

Related Commands

Command	Description
parameter-map type cws	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

outgoing

To configure filtering for outgoing export traffic, use the **outgoing** command in router IP traffic export (RITE) configuration mode. To disable filtering for outgoing traffic, use the **no** form of this command.

outgoing {**access-list** {*standard*| *extended*| *named*}| **sample one-in-every** *packet-number*}

no outgoing {**access-list** {*standard*| *extended*| *named*}| **sample one-in-every** *packet-number*}

Syntax Description

access-list *standard* | *extended named*	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic.
sample one-in-every *packet-number*	Export only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets.

Command Default

If this command is not enabled, outgoing IP traffic is not exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for IP traffic export, you can issue the **outgoing** command to filter unwanted outgoing traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Note If you issue this command, you must also issue the **bidirectional** command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming IP traffic.

pac key through port-misuse

pac key

To specify the Protected Access Credential (PAC) encryption key, use the **pac key** command in RADIUS server configuration mode. To delete the PAC key, use the **no** form of this command.

pac key *encryption-key*

no pac key *encryption-key*

Syntax Description

encryption-key	The *encryption-key* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Command Default

No PAC encryption key is specified.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

Both the **radius server** command, which enters RADIUS server configuration mode, and the **aaa new-model** command must be configured before accessing this command.

The configuration of the **pac key** command allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC's peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

In seed devices, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to configure the RADIUS server accounting and authentication parameters for PAC provisioning and the specification of the PAC key:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server
Device(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812
Device(config-radius-server)# pac key 7 mypackey
```

Related Commands

Command	Description
aaa new-model	Enables new RADIUS and AAA access control commands and functions and disables old commands.
address ipv4	Configures the RADIUS server accounting and authentication parameters for PAC provisioning.
password encryption aes	Enables a type 6 encrypted preshared key.
radius server	Specifies the name for the RADIUS server configuration for PAC provisioning and enters RADIUS server configuration mode.

parameter

To specify parameters for an enrollment profile, use the **parameter** command in ca-profile-enroll configuration mode. To disable specified parameters, use the **no** form of this command.

parameter *number* {**value** *value*| **prompt** *string*}

no parameter *number* {**value** *value*| **prompt** *string*}

Syntax Description

number	User parameters. Valid values range from 1 to 8.
value *value*	To be used if the parameter has a constant value.
prompt *string*	To be used if the parameter is supplied after the **crypto ca authenticate** command or the **crypto ca enroll** command has been entered. **Note** The value of the *string* argument does not have an effect on the value that is used by the router.

Command Default

No enrollment profile paramters are specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **parameter** command can be used within an enrollment profile after the **authentication command**commandorthe **enrollment command** has been enabled.

Examples

The following example shows how to specify parameters for the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
```

```
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
authentication command	Specifies the HTTP command that is sent to the CA for authentication.
crypto ca profile enrollment	Defines an enrollment profile.
enrollment command	Specifies the HTTP command that is sent to the CA for enrollment.

parameter-map type

To create or modify a parameter map, use the **parameter-map type**command in global configuration mode. To delete a parameter map from the configuration, use the **no** form of this command.

parameter-map type {**inspect| urlfilter| protocol-info| consent**} *parameter-map-name*

no parameter-map type {**inspect| urlfilter| protocol-info| consent**} *parameter-map-name*

Syntax Description

inspect	Defines an inspect type parameter map, which configures connection thresholds, timeouts, and other parameters pertaining to the **inspect** action.
urlfilter	Defines a URL-filter-specific parameter map.
protocol-info	Defines an application-specific parameter map. **Note** Protocol-specific parameter maps can be created only for Instant Messenger (IM) applications (AOL, I Seek You (ICQ), MSN Messenger, Yahoo Messenger and Windows Messenger).
consent	Defines an authentication proxy consent parameter map.
parameter-map-name	Name of the parameter map.

Command Default

None

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **protocol-info** keyword was added.
12.4(15)T	The **consent** keyword was added.
12.4(20)T	Support for ICQ and Windows Messenger was added.

Usage Guidelines

A parameter map allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.

There are currently four types of parameter maps:

- Inspect parameter map

An inspect parameter map is optional. If you do not configure a parameter map, the software uses default parameters. Parameters associated with the inspect action apply to all nested actions (if any). If parameters are specified in both the top and lower levels, those in the lower levels override those in the top levels.

- URL filter parameter map

A parameter map is required for URL filtering (via the URL filter action in a Layer 3 or Layer 4 policy map and the URL filter parameter map).

- Protocol-specific parameter map

A parameter map is required for an IM application (Layer 7) policy map.

- Authentication proxy consent-specific parameter map.

Examples

The following example shows how to configure an IM-based firewall policy. In this example, all Yahoo Messenger and ICQ traffic is allowed to pass through, while all MSN Messenger, AOL and Windows Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and ICQ traffic on a more granular level.

```
!
!
parameter-map type protocol-info ymsgr-servers
 server name messenger.yahoo.akadns.net
 server name .*.yahoo.com snoop
 server ip 192.0.2.100
 server ip range 192.0.2.115 192.0.2.180
parameter-map type protocol-info icq-servers
 server name login.oscar.aol.com
 server name .*.aol.com snoop
 server ip 192.0.2.200
 server ip range 192.0.2.215 192.0.2.230
!
!
class-map type inspect match-all l4-cmap-ymsgr
 match protocol ymsgr ymsgr-servers
class-map type inspect ymsgr match-any l7-cmap-ymsgr
 match  service text-chat
class-map type inspect match-all l4-cmap-icq
 match protocol icq icq-servers
class-map type inspect icq match-any l7-cmap-icq
 match  service text-chat
 match  service any
!
!
policy-map type inspect im l7-pmap-ymsgr
 class type inspect ymsgr l7-cmap-ymsgr
  allow
  log
policy-map type inspect im l7-pmap-icq
 class type inspect icq l7-cmap-icq
  allow
  log
```

```
policy-map type inspect to_internet
 class type inspect l4-cmap-ymsgr
  inspect
  service-policy im l7-pmap-ymsgr
 class type inspect l4-cmap-icq
  inspect
  service-policy im l7-pmap-icq
 class class-default
  drop
!
!
```

The following example shows a typical URL filter parameter map configuration:

```
parameter-map type urlfilter eng-filter-profile
 server vendor n2h2 172.16.1.2 port 3128 outside log timeout 10 retrans 6
 max-request 80
 max-resp-pak 200
 cache 200
 exclusive-domain permit cisco.com
 exclusive-domain deny gaming.com
```

The following example shows a sample inspect type parameter map configuration:

```
parameter-map type inspect eng_network_profile
 audit-trail on
 alert off
 max-incomplete low 2000
 max-incomplete high 3000
 one-minute low 5000
 one-minute high 8000
 udp idle-time 75
 dns-timeout 25
 tcp idle-time 90
 tcp finwait-time 20
 tcp synwait-time 10
 tcp block-non-session
 tcp max-incomplete host 2000 block-time 120
```

The following example shows how to define the consent-specific parameter map “consent_parameter_map” and a default consent parameter map:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

parameter-map type content-scan global

Note Effective with Cisco IOS Release 15.4(2)T, the **parameter-map type content-scan global** command is replaced by the **parameter-map type cws global** command. See the **parameter-map type cws global** command for more information.

To configure a global content-scan parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type content-scan global** command in global configuration mode. To delete a global content-scan parameter map, use the **no** form of this command.

parameter-map type content-scan global

no parameter-map type content-scan global

Syntax Description

This command has no arguments or keywords.

Command Default

A global content-scan parameter map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.4(2)T	This command was replaced by the **parameter-map type cws global** command.

Usage Guidelines

When you configure the **content-scan out** command on an interface, the global content-scan parameter map is also applied to that interface.

Examples

The following example shows how to configure a global content-scan parameter map:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)#
```

Related Commands

Command	Description
content-scan out	Enables content scanning on an egress interface.

parameter-map type cws global

To configure a global Cloud Web Security parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type cws global** command in global configuration mode. To delete a global Cloud Web Security parameter map, use the **no** form of this command.

parameter-map type cws global

no parameter-map type cws global

Syntax Description

This command has no arguments or keywords.

Command Default

A global content-scan parameter map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.4(2)T	This command was introduced. This command replaces the **parameter-map type content-scan global** command.

Usage Guidelines

When you configure the **cws out** command on an interface, the global Cloud Web Security parameter map is also applied to that interface.

Examples

The following example shows how to configure a global Cloud Web Security parameter map:

```
Device(config)# parameter-map type cws global
Device(config-profile)#
```

Related Commands

Command	Description
cws out	Enables Cloud Web Security content scanning on an egress interface.

parameter-map type inspect

To configure an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action, use the **parameter-map type inspect** command in global configuration mode. To delete an inspect-type parameter map, use the **no** form of this command.

parameter-map type inspect {*parameter-map-name*| **global**| **default**}

no parameter-map type inspect {*parameter-map-name*| **global**| **default**}

Syntax Description

parameter-map-name	Name of the inspect parameter map.
global	Defines a global inspect parameter map.
default	Defines a default inspect parameter map.

Command Default

No inspect-type parameter maps are set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The keywords **global** and **default** were added.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

After you enter the **parameter-map type inspect** command, you can enter the commands listed in the table below in parameter-map type inspect configuration mode.

Command	Description
alert {**on** | **off**}	Enables Cisco IOS stateful packet inspection alert messages.
audit-trail {**on** | **off**}	Enables and disables audit trail messages.

Command	Description
dns-timeout *seconds*	Specifies the Domain Name System (DNS) idle timeout.
gtp	Configures the inspection parameters for General Packet Radio Service (GPRS) Tunneling Protocol (GTP).
icmp idle-timeout *seconds*	Configures the timeout for Internet Control Message Protocol (ICMP) sessions.
max-incomplete {**low** | **high**} *number-of-connections*	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
one-minute {**low** | **high**} *number-of-connections*	Defines the rate of new half-open session initiation in one minute that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
tcp finwait-time *seconds*	Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange.
tcp idle-time *seconds*	Configures the timeout for TCP sessions.
tcp max-incomplete host *threshold* [**block-time** *minutes*}	Specifies threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention.
tcp synwait-time *seconds*	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.
udp idle-time *seconds*	Configures the timeout of UDP sessions going through the firewall.

For more detailed information about these commands, see their individual command descriptions.

Examples

The following example shows a sample inspect parameter map with the Cisco IOS stateful packet inspection alert messages enabled:

```
parameter-map type inspect eng-network-profile
 alert on
```

The following example shows a sample inspect type parameter map configuration:

```
parameter-map type inspect eng_network_profile
 audit-trail on
 alert on
 max-incomplete low unlimited
```

```
max-incomplete high unlimited
one-minute low unlimited
one-minute high unlimited
udp idle-time 30
icmp idle-time 10
dns-timeout 5
tcp idle-time 3600
tcp finwait-time 5
tcp synwait-time 30
tcp block-non-session
tcp max-incomplete host 1-2147483647 block-time unlimited
sessions maximum:2147483647
```

Related Commands

Command	Description
alert	Turns on Cisco IOS stateful packet inspection alert messages.
audit-trail	Turns audit trail messages on and off.
dns-timeout	Specifies the DNS idle timeout.
gtp	Configures the inspection parameters for GTP.
icmp idle-timeout	Configures the timeout for ICMP sessions.
inspect	Enables Cisco IOS stateful packet inspection.
max-incomplete	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
ipv6 routing-enforcement-header loose	Provides backward compatibility with the legacy IPv6 inspection.
one-minute	Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
tcp finwait-time	Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN exchange.
tcp idle-time	Configures the timeout for TCP sessions.
tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.
udp idle-time	Configures the timeout of UDP sessions going through the firewall.

parameter-map type inspect-global

To configure a global parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type inspect-global** command in global configuration mode. To delete a global parameter map, use the **no** form of this command.

parameter-map type inspect-global [**gtp**]

no parameter-map type inspect-global [**gtp**]

Syntax Description

gtp	(Optional) Specifies the General Packet Radio Service (GPRS) Tunneling Protocol (GTP).

Command Default

Global parameter maps are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **gtp** keyword was added.

Usage Guidelines

When you configure the **parameter-map type inspect-global** command, the default VPN routing and forwarding (VRF) instance gets bound to the default VRF. Use the **parameter-map type inspect-global** command to enter parameter-map type inspect configuration mode and make changes to existing configurations or to configure features like aggressive aging on the default VRF.

You cannot configure the **parameter-map type inspect global** command and the **parameter-map type inspect-global** command simultaneously. The device will accept only one of these commands.

Note The **parameter-map type inspect-global** will replace the **parameter-map type inspect global** in a future release.

You need to configure the global VRF (also known as the default VRF) by using the **parameter-map type inspect-global vrf** command and the per-box (box refers to the entire firewall session table) configuration by using the **per-box** command, after configuring the **parameter-map type inspect global** command. However, when you configure the **parameter-map type inspect-global** command, the global VRF is bound to the inspect-VRF parameter map by default.

Examples

The following example shows how to configure a global parameter map and enter parameter-map type inspect configuration mode:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)#
```

Related Commands

Command	Description
aggressive-aging	Enables aggressive aging of half-opened firewall sessions.
alert	Enables stateful packet inspection alert messages.
inspect	Enables stateful packet inspection.
log	Logs the firewall activity for an inspect parameter map.
max-incomplete	Configures the half-opened session limit for a VRF.
parameter-map type inspect global	Defines a global inspect-type parameter map.
show parameter-map type inspect-global	Displays global parameter map information.
tcp syn-flood limit	Configures a limit to the number of TCP half-opened sessions before triggering SYN cookie processing for new SYN packets.

parameter-map type inspect-vrf

To configure an inspect VPN Routing and Forwarding (VRF)-type parameter map, use the **parameter-map type inspect-vrf** command in global configuration mode. To delete an inspect VRF type parameter map, use the **no** form of this command.

parameter-map type inspect-vrf *vrf-pmap-name*

no parameter-map type inspect-vrf *vrf-pmap-name*

Syntax Description

vrf-pmap-name	Name of the parameter map.

Command Default

An inspect VRF-type parameter map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to configure an inspect VRF-type parameter map named inspect-pmap:

```
Router(config)# parameter-map type inspect-vrf inspect-pmap
```

Related Commands

Command	Description
parameter-map type	Creates or modifies a parameter map.
show parameter-map type inspect-vrf	Displays information about the configured inspect VRF-type parameter maps.

parameter-map type inspect-zone

To configure an inspect zone-type parameter map, use the **parameter-map type inspect-zone** command in global configuration mode. To remove an inspect zone type parameter map, use the **no** form of this command.

parameter-map type inspect-zone *zone-pmap-name*

no parameter-map type inspect-zone *zone-pmap-name*

Syntax Description

zone-pmap-name	Name of the parameter map.

Command Default

Inspect zone-type parameter maps are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following example shows how to create an inspect zone-type parameter map named zone-pmap:

```
Router(config)# parameter-map type inspect-zone zone-pmap
```

Related Commands

Command	Description
parameter-map type	Creates or modifies a parameter map.
show parameter-map type inspect-zone	Displays information about the configured inspect zone-type parameter maps.

parameter-map type mitigation

To configure a mitigation type parameter map for Transitory Messaging Services (TMS), use the **parameter-map** command in global configuration mode. To remove the parameter map from the router configuration file, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **parameter-map** command is not available in Cisco IOS software.

parameter-map type mitigation *name*

no parameter-map type mitigation *name*

Syntax Description

name	The name of the mitigation type parameter map.

Command Default

A mitigation type parameter map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The mitigation type parameter map is a container for TMS Rules Engine configuration parameters. The mitigation parameter map is configured on the consumer. Entering the **parameter-map type mitigation** command places the router in parameter-map configuration mode.

The mitigation type parameter map contains the next-hop variable in the mitigation type service policy (TMS Rules Engine configuration). The Rules Engine is a flexible mechanism that allows you to apply a rule on only a single consumer or to override an enforcement action sent from the controller. You can configure an enforcement action to route traffic to a null interface (black hole), route traffic to a specific interface for collection and analysis, or configure a nonstandard primitive.

Note Nonstandard primitives are predefined in the threat definition file that is loaded on the controller.

Configuring a Mitigation Type Service Policy (TMS Rules Engine Configuration)

A mitigation type service policy is created by configuring and linking mitigation type parameter and class maps to a mitigation type policy map. The mitigation type class map is configured to define threat primitive and priority traffic matching conditions. The mitigation type parameter map is configured to apply a next-hop variable to the class of traffic. The class and parameter maps are attached to a mitigation type policy map. The mitigation type service policy is activated by attaching the mitigation type policy map to a TMS type policy map, which is attached to the global consumer process.

Examples

Examples

The following example configures the TMS Rules Engine to set the next hop variable to 192.168.1.1 for traffic that matches the mitigation class (priority 1 traffic and any primitive):

```
Router(config)# class-map type control mitigation match-all MIT_CLASS_1
Router(config-cmap)# match primitive any
Router(config-cmap)# match priority 1
Router(config-cmap)# exit
Router(config)#
parameter-map type mitigation MIT_PAR_1
Router(config-profile)# variable COLLECTION ipv4 192.168.1.1
Router(config-profile)# exit
Router(config)# policy-map type control mitigation MIT_POL_1
Router(config-pmap)# class MIT_CLASS_1
Router(config-pmap-c)# source parameter MIT_PAR_1
Router(config-pmap-c)# end
```

Examples

The following example configures the TMS Rules Engine to send priority 5 redirect threat mitigation traffic to a null interface (black hole):

```
Router(config)# parameter-map type mitigation MIT_PAR_2
Router(config-profile)# variable RTBH NULL0
Router(config-profile)# exit
Router(config)# class-map type control mitigation match-all MIT_CLASS_2
Router(config-cmap)# match priority 5
Router(config-cmap)# match primitive redirect
Router(config-cmap)# exit
Router(config)# policy-map type control mitigation MIT_POL_2
Router(config-pmap)# class MIT_CLASS_2
Router(config-pmap-c)# source parameter MIT_PAR_2
Router(config-pmap-c)# redirect route $RTBH
Router(config-pmap-c)# end
```

Related Commands

Command	Description
acl drop	Configures an ACL drop enforcement action in a TMS Rules Engine configuration.
class-map type control mitigation	Configures a mitigation type class map.
ignore (TMS)	Configures the TMS Rules Engine to ignore a mitigation enforcement action.
match primitive	Configures a primitive match in a mitigation type class map.

Command	Description
match priority	Configures the match priority level for a mitigation enforcement action.
policy-map type control mitigation	Configures a mitigation type policy map.
redirect route	Configures a redirect enforcement action in a mitigation type policy map.
source parameter	Attaches a mitigation type parameter map to a policy-map class configuration.
tms-class	Associates an interface with an ACL drop enforcement action.
variable	Defines the next-hop variable in a mitigation type parameter map.

parameter-map type ooo global

To configure an Out-of-Order (OoO) global parameter map for all firewall policies, use the **parameter-map type ooo global** command in global configuration mode. To remove an OoO global parameter map, use the **no** form of this command.

parameter-map type ooo global

no parameter-map type ooo global

Syntax Description

This command has no arguments or keywords.

Command Default

OoO global parameter maps are not configured for firewall policies.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

OoO packet-processing support for the Common Classification Engine (CCE) firewall application and CCE adoptions of the Cisco Intrusion Prevention System (IPS) allows packets that arrive out of order to be copied and reassembled in the correct order. OoO packet processing reduces the need to retransmit dropped packets and reduces the bandwidth needed for the transmission of traffic on a network.

OoO packets are dropped when Cisco IPS and the zone-based policy firewall with Layer 4 inspection are enabled.

Examples

The following example shows how to configure an OoO global parameter map:

```
Device# configure terminal
Device(config)# parameter-map type ooo global
Device(config-profile)#
```

Related Commands

show parameter-map type ooo global	Displays OoO global parameter-map information.
tcp reassembly	Changes the default parameters for OoO queue processing of TCP sessions.
tcp reassembly memory limit	Specifies the limit of the OoO queue size for TCP sessions.

parameter-map type protocol-info

To create or modify a protocol-specific parameter map and enter parameter-map type configuration mode, use the **parameter-map type protocol-info**command in global configuration mode. To delete a protocol-specific parameter map from the configuration, use the **no** form of this command.

parameter-map type protocol-info [**msrpc**| **sip**| **stun-ice**] *parameter-map-name*

no parameter-map type protocol-info [**msrpc**| **sip**| **stun-ice**] *parameter-map-name*

Syntax Description

msrpc	(Optional) Defines a Microsoft Remote Procedure Call (MSRPC) protocol-info parameter map.
sip	(Optional) Defines a Session Initiation Protocol (SIP) protocol-info parameter map.
stun-ice	(Optional) Defines a Session Traversal Utilities for Network Address Translation (NAT) and Interactive Connectivity Establishment (STUN-ICE) protocol-info parameter map.
parameter-map-name	Name of the parameter map.

Command Default

No protocol-specific parameter maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.0(1)M	This command was modified. The **sip** keyword was added.
15.1(4)M	This command was modified. The **msrpc** keyword was added.

Usage Guidelines

A protocol-specific parameter map allows you to specify the parameters that control the behavior of actions specified under a policy map and match criteria specified under a class map.

Protocol-specific parameter maps can be created for real-time voice, video, and text messaging applications (such as AOL, MSN Messenger, or Windows Messenger).

Examples

The following example shows a sample SIP protocol type parameter map configuration. In this example, the parameter map is configured to not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info sip pmap-sip
Router(config-profile)# disable open-media channel
```

The following example shows a sample STUN-ICE protocol type parameter map configuration. In this example, the parameter map is configured to not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info stun-ice
Router(config-profile)# disable open-media channel
Router(config-profile)# authorization agent-id 20 shared-secret 12345flower12345
 cat-window 15
```

The following example shows how to configure an Instant Messaging-based firewall policy. In this example, all Yahoo Messenger and I Seek You (ICQ) traffic is allowed to pass through, while all MSN Messenger, AOL, and Windows Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and ICQ traffic on a more granular level.

```
Router(config)# parameter-map type protocol-info ymsgr-servers
Router(config-profile)# server name messenger.yahoo.akadns.net
Router(config-profile)# server name .*.yahoo.com snoop
Router(config-profile)# server ip 192.0.2.100
Router(config-profile)# server ip range 192.0.2.115 192.0.2.180
Router(config-profile)# exit
Router(config)# parameter-map type protocol-info icq-servers
Router(config-profile)# server name login.oscar.aol.com
Router(config-profile)# server name .*.aol.com snoop
Router(config-profile)# server ip 192.0.2.200
Router(config-profile)# server ip range 192.0.2.215 192.0.2.230
Router(config-profile)# exit
Router(config)# class-map type inspect match-all l4-cmap-ymsgr
Router(config-cmap)# match protocol ymsgr ymsgr-servers
Router(config-cmap)# exit
Router(config)# class-map type inspect ymsgr match-any l7-cmap-ymsgr
Router(config-cmap)# match  service text-chat

Router(config-cmap)# exit
Router(config)# class-map type inspect match-all l4-cmap-icq
Router(config-cmap)# match protocol icq icq-servers
Router(config-cmap)# exit
Router(config)# class-map type inspect icq match-any l7-cmap-icq
Router(config-cmap)# match  service text-chat
Router(config-cmap)# match  service any

Router(config-cmap)# exit
Router(config)# policy-map type inspect im l7-pmap-ymsgr
Router(config-pmap)# class type inspect ymsgr l7-cmap-ymsgr
Router(config-pmap-c)# allow
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config)# policy-map type inspect im l7-pmap-icq
Router(config-pmap)#class type inspect icq l7-cmap-icq
Router(config-pmap-c)# allow
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config)# policy-map type inspect to_internet
Router(config-pmap)# class type inspect l4-cmap-ymsgr
Router(config-pmap-c)# inspect

Router(config-pmap-c)# service-policy im l7-pmap-ymsgr
Router(config-pmap-c)# exit
Router(config-pmap)# class type inspect l4-cmap-icq
Router(config-pmap-c)# inspect
```

```
Router(config-pmap-c)# service-policy im l7-pmap-icq
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop
```

Related Commands

Command	Description
disable open-media-channel	Prevents the creation of RTP or RTCP media channels when a SIP class map is used for SIP inspection.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

parameter-map type regex

To configure a parameter-map type to match a specific traffic pattern, use the **parameter-map type regex** command in global configuration mode. To delete a parameter-map type with a regular expression (regex), use the **no** form of this command.

parameter-map type regex *parameter-map-name*

no parameter-map type regex

Syntax Description

parameter-map-name	Name of the parameter map. The name can have a maximum of 228 alphanumeric characters. **Note** The use of blank spaces is not recommended. The system interprets the first blank space as the end of the parameter-map name unless the string is delimited by quotation marks.

Command Default

A regex parameter map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

You can enter a regex to match text strings either literally as an exact string or by using metacharacters to match multiple variants of a text string. You can use a regex to match the content of certain application traffic; for example, you can match a uniform resource identifier (URI) string inside an HTTP packet using the **match request regex** command under an HTTP inspection class map.

Use Ctrl-V to ignore all of the special characters in the CLI, such as a question mark (?) or a tab. For example, type **d**[**Ctrl-V**]**g** to enter **d?g** in the configuration.

The table below lists the metacharacters that have special meanings.

Table 4: regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters.
(*xxx* **)**	Subexpression	A subexpression segregates characters from surrounding characters so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either of the expressions that it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl-V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1, or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least one occurrence of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{ *x* }	Repeat quantifier	Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.

Character	Description	Notes
{ *x* ,}	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc* **]**	Character class	Matches any character in the bracket. For example, **[abc]** matches a, b, or c.
[^ *abc* **]**	Negated character class	Matches a single character that is not contained within brackets. For example, **[^abc]** matches any character other than a, b, or c; and **[^A-Z]** matches any single character that is not an uppercase letter.
[*a* **-** *c*]	Character range class	Matches any character in the specified range. **[a-z]** matches any lowercase letter. You can mix characters and ranges; for example, **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does **[a-cq-z]**. **Note** The dash (-) character is literal only if it is the last or the first character within the brackets, **[abc-]** or **[-abc]**.
" "	Quotation marks	Preserves trailing or leading spaces in the string. For example, "**test**" preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When preceding a literal character, it matches the literal character. For example, **\[**matches the left square bracket.
char	Character	When the character is not a metacharacter, it matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	New line	Matches a new line 0x0a.

Character	Description	Notes
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x *nn*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal numbers (exactly two digits).
\ *nnn*	Escaped octal number	Matches an ASCII character as an octal number (exactly three digits). For example, the character 040 represents a space.

Examples

The following example shows how to configure and apply a regex parameter map to an HTTP application firewall parameter-map type whose URI matches any of the following regular expressions:

- ".*cmd.exe"
- ".*money"
- ".*shopping"

```
Router# configure terminal
Router(config)# parameter-map type regex uri-regex-cm
Router(config-profile)# pattern ".*cmd.exe"
Router(config-profile)# pattern ".*money"
Router(config-profile)# pattern ".*shopping"
Router(config-profile)# exit
Router(config)# class-map type inspect http uri-check-cm
Router(config-cmap)# match request uri regex uri-regex-cm
Router(config-cmap)# exit
Router(config)# policy-map type inspect http uri-check-pm
Router(config-pmap)# class type inspect http uri-check-cm
Router(config-pmap-c)# reset
```

The following example shows how to configure a regex parameter map whose case-insensitive pattern matches multiple variants of the string "hello":

```
Router# configure terminal
Router(config)# parameter-map type regex body_regex
Router(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
Router(config-profile)# end
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type class map.
class type inspect	Specifies the traffic (class) on which an action is to be performed.

Command	Description
match request regex	Configures an HTTP firewall policy to permit or deny HTTP traffic on the basis of request messages whose URI or arguments (parameters) match a defined regular expression.
parameter-map type	Creates or modifies a parameter map.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect-type policy map.

parameter-map type trend-global

To create or modify the parameter map for global parameters associated with a Trend Router Provisioning Server (TRPS) and to place the system in parameter map configuration mode, use the **parameter-map type trend-global** command in global configuration mode. To delete the global parameters associated with a TRPS from the configuration, use the **no** form of this command.

parameter-map type trend-global *parameter-map-name*

no parameter-map type trend-global *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map for the global parameters associated with the TRPS.

Command Default

No parameter map for the global TRPS parameters is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.1(2)T	This command was modified. The **pipeline**, **on**, and **off**keywords were added.

Usage Guidelines

Use the **parameter-map type trend-global**command to specify global parameters for the TRPS. You can specify only one trend-global parameter map on the system. To specify per-policy parameters, use the **parameter-map type urlfpolicy** command.

When you create or modify a global TRPS parameter map, use the following commands in parameter map configuration mode to set the values for the global TRPS parameters:

- **alert** {**on** | **off**}--Turns on or off URL-filtering server alert messages that are displayed on the console. The default is **on**.
- **cache-entry-lifetime** *hours* -- Specifies how long, in hours, an entry remains in the cache table. Cache entries remain in the table until the cache-entry-lifetime value for the entry expires or until the cache is full, whichever occurs first. When the cache is full, the entry is removed to make room for subsequent entries. The range is from 1 to 120. The default is 24.
- **cache-size maximum-memory** *kilobyte* -- Specifies the maximum size of the categorization cache, in kilobytes. The range is from 0 to 128000. The default is 256.

- **exit** --Exits from the parameter map.
- **no** --Negates or sets default values for a command.
- **server** {*server-name* | *ip-address*} [**http-port** *port-number*] [**https-port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*] [**pipeline** {**on** | **off**}]--Specifies information about the TRPS. Use the server command in profile configuration mode.
  - **http-port** *port-number*--Specifies the HTTP port that is listening for requests. The range is from 1 to 65535. The default is 80.
  - **https-port** *port-number*--Specifies the HTTPS port that is listening for secure HTTP requests. The range is from 1 to 65535. The default is 443.
  - **pipeline** {**on** | **off**}--Turns on or off the TRPS pipeline requests. The default is **on**.
  - **retrans** *retransmission-count*--Specifies the number of times the router retransmits the lookup request when a response is not received from the TRPS. The range is from 1 to 5. The default is 3.
  - **server** {*server-name* | *ip-address*}--Specifies the domain name or the IP address of the server. The default is trps.trendmicro.com.
  - **timeout** *seconds*--Specifies the number of seconds that the router waits for a response from the TRPS. The range is from 1 to 300. The default is 60.

Examples

The following shows an example of how to specify global TRPS parameters in a parameter map named global-parameter-map:

```
parameter-map type trend-global global-parameter-map
 server server.example.com retrans 5 timeout 200
 cache-size maximum-memory 128000
 cache-entry-lifetime 1
```

Related Commands

Command	Description
alert	Turns on or off URL-filtering system alert messages that are displayed on the console.
cache-entry lifetime	Specifies how long an entry remains in the cache table.
cache-size maximum-memory	Specifies the size of the categorization cache.
parameter-map type urlfpolicy	Specifies per-policy URL filtering parameters.
server	Specifies information about the TRPS.

parameter-map type urlfilter

Note This command is hidden in releases later than Cisco IOS Release 12.4(20)T, but it continues to work. The **parameter-map type urlfpolicy** command can also be used. This command is used to create URL filtering parameters for local, trend, Websense Internet filtering, and the N2H2 Internet blocking program. We recommend the use of the URL filter policy rather than the URL filter action for Cisco IOS Release 12.4(20)T. All the use-cases supported by URL filter as an action are also supported by URL filter policy.

To create or modify a parameter map for URL filtering parameters, use the **parameter-map type urlfilter** command in global configuration mode. To delete a URL filter parameter map, use the **no** form of this command.

parameter-map type urlfilter *parameter-map-name*

no parameter-map type urlfilter *parameter-map-name*

Syntax Description

parameter-map-name	Name of the URL parameter map.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was removed.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the following subcommands after you enter the **parameter-map type urlfilter** command. For more detailed information about the subcommands, see their individual command descriptions by going to the "Command Reference" section on page 45.

- **alert** {**on** | **off**}

Turns on or off URL-filtering system alert messages that are displayed on the console.

- **allow-mode** {**on** | **off**}

Turns on or off the default mode (allow mode) of the filtering algorithm.

- **audit-trail** {**on** | **off**}

Turns on or off the logging of URL information into the syslog server or router.

- **cache** *number-of-entries*

Configures cache parameters.

- **exclusive-domain** {**deny** | **permit**} *domain-name*

Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.

- **max-request** *number-of-requests*

Specifies the maximum number of outstanding requests that can exist at any given time.

- **max-resp-pak** *number-of-responses*

Specifies the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer.

- **server vendor** {**n2h2** | **websense**} {*ip-address* | *hostname* [**port** *port-number*]} [**outside**] [**log**] [**retrans** *retransmission-count*] [**timeout** *seconds*]

Specifies a vendor server for URL filtering.

- **source-interface** *interface-name*

Specifies the interface whose IP address will be used as the source IP address while making a TCP connection to the URL filter server (websense or N2h2).

Examples

The following example shows a sample URL parameter map:

```
parameter-map type urlfilter eng-network-profile
 server vendor n2h2 10.64.64.22 port 4128 outside retrans 4 timeout 8
```

The following example shows a typical URL filter configuration:

```
parameter-map type urlfilter eng-network-profile
 server vendor n2h2 10.64.65.22 port 3128 outside log retrans 6 timeout 10
 max-request 80
 max-resp-pak 200
 cache 200
 exclusive-domain permit cisco.com
 exclusive-domain deny gaming.com
```

Related Commands

Command	Description
alert	Turns on or off URL-filtering system alert messages that are displayed on the console.
allow-mode	Turns on or off the default mode (allow mode) of the filtering algorithm.
audit-trail	Turns on or off the logging of URL information into the syslog server or router.

Command	Description
cache	Configures cache parameters.
exclusive-domain	Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.
max-request	Specifies the maximum number of outstanding requests that can exist at any given time.
max-resp-pak	Specifies the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer.
server vendor	Specifies a vendor server for URL filtering.

parameter-map type urlfpolicy

To create or modify a parameter map for a URL filtering policy and to place the system in parameter map configuration mode, use the **parameter-map type urlfpolicy**command in global configuration mode. To delete the parameter map for a URL filtering policy from the configuration, use the **no** form of this command.

parameter-map type urlfpolicy {**local| trend| n2h2| websense**} *parameter-map-name*

no parameter-map type urlfpolicy {**local| trend| n2h2| websense**} *parameter-map-name*

Syntax Description

local	Specifies that the parameters are for a local URL filtering policy.
trend	Specifies that the parameters are for a Trend Micro URL filtering policy.
n2h2	Specifies that the parameters are for a SmartFilter (previously N2H2) URL filtering policy.
websense	Specifies that the paramaters are for a Websense URL filtering policy.
parameter-map-name	The name of the parameter map for a URL filtering policy.

Command Default

No parameter maps for a URL filtering policy are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.

Usage Guidelines

Use the **parameter-map type urlfpolicy**command to create a paramater map for a URL filtering policy. The commands that you use to specify the paramaters for a filtering policy depend on the URL filtering server you are using.

The first table below defines the parameters for a local URL filtering policy.

The second table below defines the per-policy parameters for a Trend Micro URL filtering policy. These parameters are in addition to the global Trend Micro policy parameters specified with the **parameter-map type trend-global** command.

The third table below defines the per-policy parameters for SmartFilter (N2H2) and Websense URL filtering policies.

Table 5: Parameters for Local URL Filtering Policies

Syntax	Description
alert {**on** | **off**}	Turns on or off URL filtering alert messages that are displayed on the console. The default is **off**.
allow-mode {**on** | **off**}	Specifies whether to allow or block URL requests when the URL filtering process does not have connectivity to a URL filtering database. When **allow-mode** is **on**, all unmatched URL requests are allowed; when **off**, all unmatched URL requests are blocked. The default is **off**.
block-page {**message***string* | **redirect-url***url* }	Specifies the response to a blocked URL request. • **message** *string* --Specifies the message text to be displayed when a URL request is blocked. • **redirect-url** *url* --Specifies the URL of the web page to be displayed when a URL request is blocked.
exit	Exits from the parameter map.
no	Negates or sets default values for a command.

Table 6: Parameters for Trend Micro URL Filtering Policies

Syntax	Description
allow-mode {**on** | **off**}	Specifies whether to allow or block URL requests when the URL filtering process does not have connectivity to a URL filtering database. When **allow-mode** is **on**, all unmatched URL requests are allowed; when **off**, all unmatched URL requests are blocked. The default is **off**.
block-page {**message***string* | **redirect-url***url* }	Specifies the response to a blocked URL request. • **message** *string* --Specifies the message text to be displayed when a URL request is blocked. • **redirect-url** *url* --Specifies the URL of the web page to be displayed when a URL request is blocked.

Syntax	Description
exit	Exits from the parameter map.
max-request *number-requests*	Specifies the maximum number of pending requests. The range is from 1 to 2147483647. The default is 1000.
max-resp-pak *number-responses*	Specifies the number of HTTP responses that can be buffered. The range is from 0 and 20000. The default is 200.
no	Negates or sets default values for a command.
truncate hostname	Specifies that URLs be truncated at the end of the domain name.

Table 7: Parameters for SmartFilter and Websense URL Filtering Policies

Syntax	Description
alert {**on** | **off**}	Turns on or off URL filtering alert messages that are displayed on the console. The default is **off**.
allow-mode {**on** | **off**}	Specifies whether to allow or block URL requests when the URL filtering process does not have connectivity to a URL filtering database. When **allow-mode** is **on**, all unmatched URL requests are allowed; when **off**, all unmatched URL requests are blocked. The default is **off**.
block-page {**message***string* | **redirect-url***url* }	Specifies the response to a blocked URL request. • **message** *string* --Specifies the message text to be displayed when a URL request is blocked. • **redirect-url** *url* --Specifies the URL of the web page to be displayed when a URL request is blocked.
cache-entry-lifetime *hours*	Specifies how long, in hours, an entry remains in the cache table. The default is 24.
cache-size maximum-entries *number-entries*	Specifies the maximum number of entries that can be stored in the categorization cache. The default is 5000.
exit	Exits from the parameter map.

Syntax	Description
max-request *number-requests*	Specifies the maximum number of pending requests. The range is from 1 to 2147483647. The default is 1000.
max-resp-pak *number-responses*	Specifies the number of HTTP responses that can be buffered. The range is from 0 and 20000. The default is 200.
no	Negates or sets default values for a command.
server {*server-name* | *ip-address*} [**source-interface** *interface-name*][**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]	Specifies the parameters for the URL filtering server. • **server** {*server-name* | *ip-address*} Specifies the domain name or the IP address of the URL filtering server. • [**source-interface** *interface-name*] Specifies the interface whose IP address will be used as the source IP address when a TCP connection is established between the system and the URL filtering server. • **outside** Specifies whether the URL filtering server is outside the network. • **port** *port-number* Specifies the port that is listening for requests. The range is from 1 to 65535. The default is 80. • **retrans** *retransmission-count* Specifies the number of times the Cisco IOS firewall retransmits the lookup request when a response is not received from the Trend Router Provisioning Server (TRPS). The range is from 1 to 5. The default is 3. • **timeout** *seconds* Specifies the number of seconds that the Cisco IOS firewall waits for a response from the TRPS. The range is from 1 to 300. The default is 60.

Syntax	Description
truncate {hostname | script-options}	Specifies that URLs be truncated. • **hostname** Specifies that URLs be truncated at the end of the domain name. • **script-options** Specifies that URLs be truncated at the left-most question mark in the URL.
urlf-server-log {on | off}	Enables sending information about HTTP requests to the URL filtering server's log server. The information includes the URL, the hostname, the source IP address, and the destination IP address.

Examples

The following example shows a parameter map for a local URL filtering policy that does not send alert messages and displays the message "URL is blocked by local filters" when a URL is blocked:

```
parameter-map type urlfpolicy local local-param-map
 alert off
 block-page message "URL is blocked by local-filters"
```

The following example shows a configuration for global parameters and per-policy parameters for a Trend Micro URL filtering policy:

```
parameter-map type trend-global global-param-map
 server mytrps.trendmicro.com retrans 5 timeout 200
 cache-size maximum-memory 128000
 cache-entry-lifetime 1
parameter-map type urlfpolicy trend trend-param-map
 max-request 2147483647
 max-resp-pak 20000
 truncate hostname
 block-page message "group2 is blocked by trend"
```

The following example shows the configuration for per-policy parameters for a SmartFilter URL filtering policy:

```
parameter-map type urlfpolicy n2h2 n2h2-param-map
 server n2h2Server timeout 30
 max-request 2000
 max-resp-pak 2000
 source-interface Loopback0
 truncate script-parameters
 cache-size maximum-entries 100
 cache-entry-lifetime 1
 block-page redirect-url http://www.example.com
```

Related Commands

Command	Description
parameter-type trend-global	Specifies the global parameters associated with Trend Micro URL filtering policies.

parameter-map type urlf-glob

To create or modify a parameter map used to specify a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering, use the parameter-map type urlf-glob command in global configuration mode. To delete the parameter map, use the no form of this command.

parameter-map type urlf-glob *parameter-map-name*

no parameter-map type urlf-glob *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map for a local URL filtering policy.

Command Default

No URL filtering parameter maps are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The parameter-map type urlf-glob command can be used to create a parameter map for trusted domains, a parameter map for untrusted domains, and a parameter map for URL keywords. The following sub-commands are available in parameter map configuration mode to specify matching parameters when the parameter-map type urlf-glob command is issued:

- exit--Exits from URL filtering parameter map configuration mode.
- no--Negates or sets default values for a command.
- pattern expression--Configures a matching pattern that refers to a domain name, URL keyword, URL metacharacter entry, or URL keyword and URL metacharacter combination. The characters /, {, and } are not allowed in the expression. The question mark (?) is not allowed because it is reserved for the help function in the command-line interface (CLI).

URL pattern matching is improved because the period (.) is interpreted as a dot, and not as a wildcard entry representing a single character, as is the case with regex regular expression pattern matching.

A URL keyword is a complete word that occurs after the domain name and that is between the forward slash (/) path delimiters. For example in the URL http://www.example.com/hack/123.html, only “hack” and “123.html” are treated as keywords. Anything in the host or domain name can be allowed or blocked using a domain name, and thus a URL keyword should be a word that comes after the domain name. The entire keyword in

the URL must match the pattern. For example if you have pattern hack, the URL www.example.com/hacksite/123.html doesn't match the pattern. In order to match this URL, you must have hacksite.

URL metacharacters allow pattern matching of single characters or ranges of characters to URLs, similar to the way a UNIX style glob expression works. The URL metacharacters are presented in the table below.

Table 8: URL Metacharacters for URL Pattern Matching

Character	Description
*	Asterisk--matches any sequence of 0 or more characters.
[*abc* **]**	Character class--matches any character in the brackets. The character matching is case sensitive. For example, **[abc]** matches a, b, or c.
[*a* **-** *c*]	Character range class. Matches any character in the range. The character matching is case sensitive. **[a-z]** matches any lowercase letter. You can mix characters and ranges; for example, **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does **[a-cq-z]**. **Note** The dash (-) character is literal only if it is the last or the first character within the brackets, **[abc-]** or **[-abc]**.
[0-9]	Numerical range class. Matches any number in the brackets. For example [0-9] matches 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.

URL metacharacters are combined with domain names and URL keywords for pattern matching. For example, pattern *.example.com will match the domain name www.example.com and pattern www.[ey]xample.com can be used to block both www.example.com and www.yxample.com. Also, pattern www.example[0-9][0-9].com can be used to block www.example01.com, www.example33.com, and www.example99.com. An example of combining a keyword and metacharacter for pattern matching is using pattern hack* to block www.example.com/hacksite/123.html.

Examples

The following shows an example of specifying the parameter map for trusted domains:

```
Router(config)# parameter-map type urlf-glob trusted-domain-param
Router(config-profile)# pattern www.example.com
Router(config-profile)# pattern *.example2.com
```

The following shows an example of a parameter map specifying keywords to be blocked:

```
Router(config)# parameter-map type urlf-glob keyword-param
Router(config-profile)# pattern example1
Router(config-profile)# pattern example3
```

The following shows an example of a parameter map specifying URL metacharacters to be blocked:

```
Router(config)# parameter-map type urlf-glob metacharacter-param
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map that specifies the traffic to which a URL filtering policy applies.
pattern (parameter-map)	Configures a matching pattern that specifies a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering.

parameter map type webauth

To define a parameter map for web authentication, use the **parameter-map type webauth** command in global configuration mode. To delete a parameter map, use the **no** form of this command.

parameter map type webauth { *parameter-map-name*| **global**}

no parameter map type webauth { *parameter-map-name*| **global**}

Syntax Description

parameter-map-name	Parameter map name for web authentication.
global	Defines global parameters for web authentication.

Command Default

A parameter map for web authentication is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.2SECisco IOS XE 3.2SECisco IOS 15.0(2)EXCisco IOS 15.0(2)EX1	This command was introduced.
Cisco IOS XE 3.6E Cisco IOS 15.2(2)E	This command was introduced.

Usage Guidelines

Use the **parameter-map type webauth** command to define a parameter map for web authentication. A parameter map allows you to specify parameters that control the behavior of actions configured under a policy map with the authenticate using **webauth** command.

A global parameter map contains system-wide parameters. This parameter map is not attached to the web authentication action and has parameters for both web authentication and consent. The global parameter map is automatically applied to the authentication action. If you explicitly apply a named parameter map, and there are parameters that are common to both the global and named parameter map, the global parameter map configuration takes precedence.

The configuration parameters supported for a global parameter map defined with the global keyword are different from the parameters supported for a named parameter map defined with the *parameter-map-name* argument.

Examples

The following example shows how to configure a parameter map named PMAP_2, which is used by the control policy named POLICY_1 to authenticate users:

```
SwitchControllerDevice(config)# parameter map type webauth global
Device(config)# parameter map type webauth global
```

parser view

To create or change a command-line interface (CLI) view and enter view configuration mode, use the **parser view** command in global configuration mode. To delete a view, use the **no** form of this command.

parser view *view-name* **[inclusive]**

no parser view *view-name* **[inclusive]**

Syntax Description

view-name	View name, which can include 1 to 30 alphanumeric characters. The *view-name* argument must not have a number as the first character; otherwise, you will receive the following error message: “Invalid view name.”
inclusive	(Optional) Specifies that all commands are included by default.

Command Default

A CLI view does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.
15.4(1)S	This command was integrated into Cisco IOS Release 15.4(1)S.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

A CLI view is a set of operational commands and configuration capabilities that restrict user access to the CLI and configuration information; that is, a view allows users to define what commands are accepted and what configuration information is visible.

After you have issued the **parser view** command, you can configure the view via the **secret 5** command and the **commands** command.

To invoke the **parser view** command, the system of the user must be set to root view. The root view can be enabled via the **enable view** command.

To create a view including all commands by default, use the **inclusive** keyword. An **inclusive-exclusive** command does not appear in other standard CLI views or in any other standard CLI inclusive views.

Note To modify the standard CLI view settings, you must delete and re-create the CLI view without the **inclusive** keyword.

Examples

The following example shows how to configure two CLI views, “first” and “second”:

```
Device(config)# parser view first inclusive
Device(config-view)# secret 5 firstpass
Device(config-view)# command exec exclude show version
Device(config-view)# command exec exclude configure terminal
Device(config-view)# command exec exclude all show ip
Device(config-view)# exit
Device(config)# parser view second
Device(config-view)# secret 5 secondpass
Device(config-view)# command exec include-exclusive show ip interface
Device(config-view)# command exec include logout
Device(config-view)# exit
```

Related Commands

Command	Description
commands (view)	Adds commands to a CLI view.
secret 5	Associates a CLI view or a superview with a password.

parser view superview

To create a superview and enter view configuration mode, use the **parser view superview** command in global configuration mode. To delete a superview, use the **no** form of this command.

parser view *superview-name* **superview**

no parser view *superview-name* **superview**

Syntax Description

superview-name	Superview name, which can include 1 to 30 alphanumeric characters. The *superview-name* argument must not have a number as the first character.

Command Default

A superview does not exist.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

A superview consists of one or more command-line interface (CLI) views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain the following characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged in to a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.

- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.

Adding CLI Views to a Superview

You can add a view to a superview only after a password has been configured for the superview (via the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.

Note Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following example shows how to create a superview (su_view1) and enter view configuration mode; two CLI views (view_one, view_two) are added to the superview also:

```
Router> enable view
Router# configure terminal
Router(config)# parser view su_view1 superview
Router(config-view)# secret 5 secret
Router(config-view)# view view_one
Router(config-view)# view view_two
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.
view	Adds a normal CLI view to a superview.

pass

To allow packets to be sent to the router without being inspected, use the **pass** command in policy-map-class configuration mode.

pass [log]

Syntax Description

log	(Optional) Logs the packets passed by the firewall pass policy.

Command Default

Traffic is not passed; that is, it is dropped.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS-XE 2.4	This command was integrated into Cisco IOS-XE Release 2.4. The **log** keyword was added.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

Examples

The following example specifies that policy map p1 passes and logs the traffic:

```
policy-map type inspect p1
 class type inspect c1
  pass log
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates a Layer 3 or Layer 4 inspect type policy map.

Command	Description
log (parameter-map type)	Logs the firewall activity for an inspect parameter map.

passive

To move a group member directly into passive mode, use the **passive** command in crypto gdoi group configuration mode. To disable the passive mode setting, use the **no** form of this command.

passive

no passive

Syntax Description

This command has no arguments or keywords.

Command Default

The group member is in full crypto send and receive mode.

Command Modes

Crypto gdoi group configuration (crypto-gdoi-group)

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

By using the **passive** command, you avoid having to use the **crypto gdoi gm ipsec direction inbound optional**privileged EXEC command, which is not persistent after a router reload and can be overriden by key server configuration from a rekey.

Examples

The following example shows that the group member group1 is being moved to passive mode:

```
crypto gdoi group group1
 identity 2345
 passive
 server address ipv4 10.34.255.57
```

Related Commands

Command	Description
crypto gdoi gm	Changes the IPsec SA status of group members.

passwd encryption

To enable or disable global AES encryption, use the **passwd encryption** command in global configuration mode. To disable password encryption, use the **no** form of this command.

passwd encryption {**on** | **off**}

no passwd encryption

Syntax Description

on	Enables password encryption.
off	Disables password encryption.

Command Default

Password keys are encrypted.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced in a release earlier than Cisco IOS XE Release 3.2SE.
15.2(2)E	This command was modified. In Cisco IOS Release 15.2(2)E and later releases, you have to configure either the **passwd key random** command or the **passwd key obfuscate** command after using the **passwd encryption on** command.

Usage Guidelines

The AES algorithm supports reversible encryption. Once the encryption is on, you must configure a method of encryption. Use the **passwd key** command to generate a password. The password module supports three types of keys - user-defined key, randomly generated key and static key.

In releases earlier than Cisco IOS Release 15.2(2)E, the **passwd encryption on** command generates an obfuscated password.

In Cisco IOS Release 15.2(2)E and later releases, ensure that you configure either the **passwd key random** command or the **passwd key obfuscate** command after using the **passwd encryption on** command.

Examples

The following example shows that an encrypted key has been enabled:

```
Device> enable
Device# configure terminal
Device(config)# passwd encryption on
```

```
Device(config)# passwd key random
Device(config)# end
```

Related Commands

Command	Description
passwd key	Manages password keys.

passwd key

To manage password keys, use the **passwd key** command in global configuration mode. To disable password generation, use the **passwd key zeroize** command.

passwd key {**ascii** | **export** | **import** | **obfuscate** | **random** | **zeroize**}

Syntax Description

ascii	Configures password or phrase to generate a key.
export	Exports the encryption key.
import	Imports the encryption key.
obfuscate	Enables password encryption using static key.
random	Configures a random encryption key.
zeroize	Deletes an encryption key.

Command Default

A static key with a fixed value is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced in a release earlier than Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **passwd encryption on** command to enable the password encryption before you generate a password.

In releases earlier than Cisco IOS Release 15.2(2)E, the **passwd encryption on** command generates an obfuscated password.

In Cisco IOS Release 15.2(2)E and later releases, ensure that you configure either the **passwd key random** command or the **passwd key obfuscate** command after using the **passwd encryption on** command.

The password module supports three types of keys - user-defined key, randomly generated key, and static key. Static keys are simple and do not require any key management. But it is not a secure option because in case the static (fixed) key is discovered, the data can be decrypted. Hence it is called obfuscation.

User-defined keys and randomly generated keys provide better security but sometimes affect the usability of a product. While using user-defined or random keys, ensure that you:

- Use the same key for the configuration data in the host and target systems.
- Reencrypt all the existing passwords using the new key in case the encryption key is updated.
- Include the key during configuration synchronization between active and standby systems so that the standby system is able to decrypt the data.

Use the **zeroize** keyword to delete the key in case the key is not secure due to leakage of encryption key or to prevent disclosure of the key. Once the key is deleted, the data encrypted by using the deleted encryption key cannot be decrypted.

Examples

The following example shows that an encrypted key has been enabled for an obfuscated password:

```
Device> enable
Device# configure terminal
Device(config)# passwd encryption on
Device(config)# passwd key obfuscate
Device(config)# end
```

Related Commands

Command	Description
passwd encryption	Enables or disables global AES encryption.

password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

password *string*

no password

Syntax Description

string	Name of the password.

Command Default

You are prompted for the password during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Before you can issue the password command, you must enable the **crypto ca trustpoint**command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example shows how to specify the password “revokeme” for the certificate request:

```
crypto ca trustpoint trustpoint1
 enrollment url http://trustpoint1.example.com/
 subject-name OU=Spiral Dept., O=example1.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokeme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

password (config-filter)

To specify the password for an authentication, authorization, and accounting (AAA) cache filter server profile, use the **password** command in AAA cache filter server configuration mode. To remove the password, use the **no** form of this command.

password [**0** | **6** | **7**] *password*

no password

Syntax Description

0	(Optional) Specifies that an unencrypted password follows.
6	(Optional) Specifies that an advanced encryption scheme (AES) encrypted password follows.
7	(Optional) Specifies that a hidden password follows.
password	The unencrypted (clear text) shared password.

Command Default

A password is not specified.

Command Modes

AAA cache filter server configuration (config-filter)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

Use the **aaa new-model** command to enable authentication, authorization, and accounting (AAA).

Before using the **password** command in AAA cache filter server configuration mode, the **aaa cache filterserver** command must be configured.

Examples

The following example shows how to specify the password "admin" for the AAA cache filter server:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization cache filterserver default cache radius
Device(config)# aaa cache filterserver
Device(config-filter)# password 0 admin
```

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.
aaa cache filterserver	Enables AAA filter server definitions.
aaa new-model	Enables the AAA access control model.

password (dot1x credentials)

To specify the password for an 802.1X credentials profile, use the **password** command in dot1x credentials configuration mode. To remove the password, use the **no** form of this command.

password [**0**| **7**] *password*

no password

Syntax Description

0	(Optional) A plain text password will follow. The default is 0.
7	(Optional) An encrypted password will follow. The default is 0.
password	The password.

Command Default

A password is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

Examples

The following example shows which credentials profile should be used when configuring a supplicant. The password is “secret.”

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface along with the **dot1x pae supplicant** command and keyword to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies the 802.1X credentials profile to be used.

password (line configuration)

To specify a password on a line, use the **password** command in line configuration mode. To remove the password, use the **no** form of this command.

password *password*

no password

Syntax Description

password	Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret.

Command Default

No password is specified.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an EXEC process is started on a line with password protection, the EXEC prompts for the password. If the user enters the correct password, the EXEC prints its normal privileged prompt. The user can try three times to enter a password before the EXEC exits and returns the terminal to the idle state.

Examples

The following example removes the password from virtual terminal lines 1 to 4:

```
line vty 1 4
 no password
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

password 5

Note Effective with Cisco IOS Release 12.3(14)T, this command is replaced by the **secret** command.

To associate a command-line interface (CLI) view or a superview with a password, use the **password 5**command in view configuration mode.

password 5 *password*

Syntax Description

password	Password for users to enter the CLI view or superview. A password can contain any combination of alphanumeric characters. **Note** The password is case sensitive.

Command Default

A user cannot access a CLI view or superview.

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	This command was enhanced to support superviews.
12.3(14)T	This command was replaced by the secret command.

Usage Guidelines

A user cannot access any commands within the CLI view or superview until the **password 5**command has been issued.

Examples

The following example show how to configure two CLI views, “first” and “second” and associate each view with a password:

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# password 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
```

```
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# password 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

password encryption aes

To enable a type 6 encrypted preshared key, use the **password encryption aes**command in global configuration mode. To disable password encryption, use the **no** form of this command.

password encryption aes

no password encryption aes

Syntax Description

This command has no arguments or keywords.

Command Default

Preshared keys are not encrypted.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption**command with the **password encryption aes**command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes**command without configuring the **key config-key password-encryption**command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

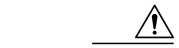
Note For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption**command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption**command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.



Caution If the password configured using the **key config-key password-encryption**command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption**command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can "read" the password (configured using the **key config-key password-encryption**command), there is no way that the password can be retrieved from the router. Existing management stations cannot "know" what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption**command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

"ciphertext>[for username bar>] is incompatible with the configured master key."
If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption**command. Deleting the master key using the **no key config-key password-encryption**command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encrypted preshared key has been enabled:

```
Router (config)# password encryption aes
```

Related Commands

Command	Description
key config-key password-encryption	Stores a type 6 encryption key in private NVRAM.
password logging	Provides a log of debugging output for a type 6 password operation.

password logging

To get a log of debugging output for a type 6 password operation, use the **password logging**command in global configuration mode. To disable the debugging, use the **no** form of this command.

password logging

no password logging

Syntax Description

This command has no arguments or keywords.

Command Default

Debug logging is not enabled.

Command Modes

Global Configuration #

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Examples

The following example shows that debug logging is configured:

```
Router# password logging
```

Related Commands

Command	Description
key config-key password-encryption	Stores an encryption key in private NVRAM.
password encryption aes	Enables a type 6 encrypted preshared key.

passthrou-domain-list name

To configure a domain name list of domains with DNS snooping, use the **passthrou-domain-list name** command in global configuration.

passthrou-domain-list *name*

Syntax Description

name	Configures the domain name list.

Command Default

None

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3E	This command was introduced.

Examples

This example shows how to configure a domain name list of domains with DNS snooping:

```
SwitchControllerDevice(config)# passthrou-domain-list name abc
SwitchControllerDevice(config-fqdn-acl-domains)# match google
```

pattern (parameter-map)

To configure a matching pattern that specifies a list of domains, URL keywords, or URL metacharacters that must be allowed or blocked by the local URL filtering, use the **pattern** command in parameter-map type inspect configuration mode. To remove the matching pattern, use the **no** form of this command.

pattern *expression*

no pattern *expression*

Syntax Description

expression	Matching pattern argument that refers to a domain name, URL keyword, URL metacharacter entry, or a URL keyword and URL metacharacter combination.

Command Default

No pattern is created for the parameter map.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

A matching pattern expression is configured for a parameter map created by the **parameter-map type regex** or the **parameter-map type urlf-glob** command.

In a pattern expression, the characters /, {, and } are not allowed. The question mark (?) character is not allowed because it is reserved for the CLI help function. The asterisk (*) character is not allowed at the beginning of a pattern.

For URL pattern matching, the period (.) character is interpreted as a dot and not as a wildcard entry that represents a single character, as is the case with regular expression pattern matching. Any character in the host or domain name can be allowed or blocked through URL filtering.

A URL keyword is a complete word that comes after the domain name and is between the forward slash (/) path delimiters. For example, in the URL http://www.example.com/hack/123.html, only “hack” is treated as a keyword. The entire keyword in the URL must match a pattern. For example, if you have configured a pattern named “hack,” the URL www.example.com/hacksite/123.html will not match the pattern. To match the URL, your pattern must have “hacksite.”

URL metacharacters allow pattern matching of single characters or ranges of characters to URLs, similar to the way a UNIX glob expression works. URL metacharacters are described in the following table.

Table 9: URL Metacharacters for URL Pattern Matching

Character	Description
*	Asterisk—matches any sequence of 0 or more characters.
[*abc* **]**	Character class—matches any character within brackets. The character matching is case sensitive. For example, **[abc]** matches a, b, or c.
[*a-c*]	Character range class—matches any character in a specified range. The character matching is case sensitive. For example, **[a-z]** matches any lowercase letter. You can also mix characters and ranges; for example, **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does **[a-cq-z]**. **Note** The dash (-) character is matched only if it is the last or the first character within brackets. For example, **[abc-]** or **[-abc]**.
[0-9]	Numerical range class—matches any number within brackets. For example, [0-9] matches 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.

URL metacharacters are combined with domain names and URL keywords for pattern matching. For example, pattern *.example.com will match the domain name www.example.com and pattern www.[ey]xample.com can be used to block both www.example.com and www.yxample.com. Also, you can use pattern www.example[0-9][0-9].com to block www.example01.com, www.example33.com, www.example99.com, and so on. You can combine a keyword and a metacharacter and create a matching pattern to block a URL. For example, you can use pattern hack* to block www.example.com/hacksite/123.html.

When you configure the **parameter-map type regex** command and then the **pattern** command, patterns that are specified in the **pattern** command are used as filters in General Packet Radio Service (GPRS) Tunneling Protocol (GTP) classes.

Examples

The following example shows how to configure a parameter map for trusted domains:

```
Device(config)# parameter-map type urlf-glob trusted-domain-param
Device(config-profile)# pattern www.example.com
Device(config-profile)# pattern *.example2.com
```

The following example shows how to configure a parameter map that specifies keywords that should be blocked:

```
Device(config)# parameter-map type urlf-glob keyword-param
Device(config-profile)# pattern example1
Device(config-profile)# pattern example3
```

The following example shows how to configure a parameter map that specifies the URL metacharacters to be blocked:

```
Device(config)# parameter-map type urlf-glob metacharacter-param
Device(config-profile)# pattern www.example[4-9].com
```

The following example shows how to specify a case-insensitive pattern that matches multiple variants of the string “hello”:

```
Device(config)# parameter-map type regex body-regex
Device(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
```

The following example shows an error message that appears on the console when an asterisk (*) character is specified at the beginning of a pattern:

```
Device(config)# parameter-map type regex gtp-map
Device(config-profile)# pattern *.gprs.com
%Invalid first char + or * in regex pattern
```

Related Commands

Command	Description
class-map type urlfilter	Creates a class map that specifies the traffic to which a URL filtering policy applies.
parameter-map type regex	Configures a regex parameter map that matches a specific regular expression pattern and enters parameter-map type inspect configuration mode.
parameter-map type urlf-glob	Creates or modifies a parameter map that specifies a list of domains, URL keywords, or URL metacharacters that should be allowed or blocked by local URL filtering and enters parameter-map type inspect configuration mode.

peer

To define a static peer for the FlexVPN client, use the **peer** command in IKEv2 FlexVPN client profile configuration mode. To remove the peer, use the **no** form of this command.

peer *sequence* {*ipv4-address*| *ipv6-address*| **fqdn** *fqdn-name* [**dynamic**| **ipv6**]} [**track** *track-number* [**up**| **down**]]

no peer *sequence*

Syntax Description

sequence	Sequence number of the peer.
ipv4-address	IPv4 address of the peer.
ipv6-address	IPv6 address of the peer.
fqdn *fqdn-name*	Assigns a fully qualified domain name (FQDN) to the peer.
dynamic	(Optional) Dynamically resolves the peer when it is chosen to connect.
ipv6	(Optional) Resolves the peer using the IPv6 address hostname.
track *track-number*	(Optional) Tracks the peer with the track number specified in the IKEv2 FlexVPN client profile.
up	(Optional) Implies that connection with the peer will be established only if track is in the up state.
down	(Optional) Implies that connection with the peer will be established only if track is in the down state.

Command Default

A static peer is not defined.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.2(3)T	This command was modified. Support for IPv6 addresses and hostnames was added.

Release	Modification
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

Peers are ordered by preference; the lower the sequence number, the higher the preference. If a peer has the same priority as an existing peer, the old peer is overridden. Sequence numbering is ideal for easy management.

If a peer is referenced by FQDN, the peer is resolved during configuration unless the **dynamic** keyword is used to resolve the peer when the peer chooses to connect.

A peer address can be used only if it can be routed in the tunnel VRF of the tunnel interface.

Examples

The following example shows how to define a static peer:

```
Device(config)# crypto ikev2 client flexvpn client1
Device(config-ikev2-flexvpn)# peer 1 10.0.0.1
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

peer address ipv4

To configure a Group Domain of Interpretation (GDOI) redundant peer key server, use the **peer address ipv4**command in GDOI redundancy configuration mode. To remove the peer key server that was configured, use the **no** form of this command.

peer address ipv4 *ip-address*

no peer address ipv4 *ip-address*

Syntax Description

ip-address	IP address of the peer key server.

Command Default

(Redundancy does not function correctly if at least one peer is not configured under the local key server configuration on a key server.)

Command Modes

GDOI redundancy configuration (gdoi-coop-ks-config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

For redundancy between key servers to operate correctly, there have to be at least two key servers in a redundant group. Therefore, at least one other peer must be defined on a key server using the **peer address ipv4** command. The local key server sets up an Internet Key Exchange (IKE) session with the peer that is defined using this command and proceeds to communicate using IKE informational messages to complete the election process using the specified IP address of the peer.

Examples

The following example shows that two peer key servers have been configured: 10.41.2.5 and 10.33.5.6.

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.
redundancy	Enters GDOI redundancy configuration mode and allows for key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

peer (IKEv2 keyring)

To define a peer or a peer group for the Internet Key Exchange Version 2 (IKEv2) keyring, use the **peer** command in IKEv2 keyring configuration mode. To remove the peer, use the **no** form of this command.

peer *name*

no peer *name*

Syntax Description

name	The peer name.

Command Default

A peer is not defined or configured.

Command Modes

IKEv2 keyring configuration (config-ikev2-keyring)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to define the name of a peer or peer group. This command enters IKEv2 keyring peer configuration mode. A peer subblock identifies a peer or peer-group using identity, hostname or address statements. A peer subblock must have atleast one statement identifying a peer or peer group. A peer subblock can have a single statement of each type identifying a peer or peer group. A peer subblock can have a single key or key-pair.

Examples

The following example shows how to configure an IKEv2 keyring with multiple peer subblocks:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(configikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1

Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
Router(configikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2
Router(config-ikev2-keyring-peer)# host peer1.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key key-2
Router(configikev2-keyring)# peer peer3
Router(config-ikev2-keyring-peer)# description peer3
Router(config-ikev2-keyring-peer)# host peer3.example.com
```

```
Router(config-ikev2-keyring-peer)# identity key-id abc
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key key-3
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
pre-shared-key **(ikev2 keyring)**	Defines a preshared key for the IKEv2 peer.

peer reactivate

To enable the reactivate primary peer feature, use the **peer reactivate** command in IKEv2 FlexVPN client profile configuration mode. To disable the feature, use the **no** form of this command

peer reactivate

no peer reactivate

Command Default

The peer reactivate feature is disabled by default.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

The peer reactivate feature provides the ability to establish connection with a new peer. If a FlexVPN client is connected to a peer with a lower priority and the track object comes UP for another peer associated with this track object having a higher priority, the existing session is brought down and the connection is established with the new peer.

For example, there are two peers: peer1 with sequence 0 associated with track1 and peer 2 with sequence 1. If the FlexVPN client is connected to peer 2 and track 1 associated with peer 1 comes up, FlexVPN client deletes the existing session and brings up a new session with peer1. If the peer reactivate feature is not configured, FlexVPN continues the session with peer 2 even though the track 1 associated with peer 1 comes up.

Note If a session with peer reactivate feature is UP and the feature is deleted, the session is not terminated. However, if a session without peer reactivate is UP and the feature is enabled, the session is terminated.

Examples

The following example shows how to enable the peer reactivate feature:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# peer reactivate
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

per-box aggressive-aging

To enable aggressive aging of all firewall sessions listed in the firewall session table (the "box"), use the **per-box aggressive-aging** command in parameter-map type inspect configuration mode. To disable the aggressive aging of global firewall sessions, use the **no** form of this command.

per-box aggressive-aging high {*value* **low** *value*| **percent** *percent* **low percent** *percent*}

no per-box aggressive-aging high {*value* **low** *value*| **percent** *percent* **low percent** *percent*}

Syntax Description

high	Specifies the high watermark for aggressive aging.
value	High watermark in absolute values. Valid values are from 1 to 4294967295.
low	Specifies the low watermark values for aggressive aging.
value	Low watermark in absolute values. Valid values are from 1 to 4294967295.
percent *percent*	Specifies the high watermark percentage for aggressive aging. Valid values are from 1 to 100.
low percent *percent*	Specifies the low watermark percentage for aggressive aging. Valid values are from 1 to 100.

Command Default

The aggressive aging of firewall sessions is not enabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The Aggressive Aging feature allows the firewall to aggressively age out sessions to make room for new sessions. Per-box aggressive aging protects the firewall session table from getting filled. When you enable aggressive aging on a router, only active sessions on the router are deleted.

You must configure the **parameter-map type inspect global** command before you configure the **per-box aggressive-aging** command.

Examples

The following example shows how to enable the aggressive aging of firewall sessions:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# per-box aggressive-aging high percent 75 low percent 35
Router(config-profile)# end
```

Related Commands

Command	Description
max-incomplete aggressive-aging	Configures the aggressive aging of half-opened firewall sessions for inspect parameter maps.
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

per-box max-incomplete

To configure the half-opened session limit for each session listed in the firewall session table (the "box"), use the **per-box max-incomplete** command in parameter-map type inspect configuration mode. To disable the configuration, use the **no** form of this command.

per-box max-incomplete [**icmp** | **tcp** | **udp**] *number*

no per-box max-incomplete [**icmp** | **tcp** | **udp**] *number*

Syntax Description

icmp	(Optional) Specifies the maximum half-opened Internet Control Message Protocol (ICMP) connections for the firewall session table.
tcp	(Optional) Specifies the maximum half-opened TCP connections for the firewall session table.
udp	(Optional) Specifies the maximum half-opened UDP connections for the firewall session table.
number	Number of half-opened sessions. Valid values are from 1 to 4294967295.

Command Default

The half-opened session limit is not set.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

A half-opened session is a session that has not reached the established state.

You must configure the **parameter-map type inspect global** command before you configure the **per-box max-incomplete** command.

Examples

The following example shows how to configure the maximum half-opened session limit to 3456:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# per-box max-incomplete 3456
Router(config-profile)# end
```

Related Commands

Command	Description
max-incomplete (inspect-vrf)	Configures the half-opened session limit for a VRF.
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

per-box max-incomplete aggressive-aging

To configure aggressive aging of half-opened firewall sessions listed in the firewall session table (the "box"), use the **per-box max-incomplete aggressive-aging** command in parameter-map type inspect configuration mode. To disable the configuration, use the **no** form of this command.

per-box max-incomplete *number* **aggressive-aging high** {*value* **low** *value*| **percent** *percent* **low percent** *value*}

no per-box max-incomplete *number* **aggressive-aging high** {*value* **low** *value*| **percent** *percent* **low percent** *value*}

Syntax Description

number	Number of half-opened sessions. Valid values are from 1 to 4294967295.
high	Specifies the high watermark for aggressive aging.
value	High watermark in absolute values. Valid values are from 1 to 4294967295.
low	Specifies the low watermark values for aggressive aging.
value	Low watermark in absolute values. Valid values are from 1 to 4294967295.
percent *percent*	Specifies the high watermark percentage for aggressive aging. Valid values are from 1 to 100.
low percent *percent*	Specifies the low watermark percentage for aggressive aging. Valid values are from 1 to 100.

Command Default

The aggressive aging of half-opened sessions is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The Aggressive Aging feature allows the firewall to aggressively age out half-opened sessions to make room for new sessions. Per-box aggressive aging protects the firewall session table from getting filled with sessions. When you enable aggressive aging on a router, only active sessions on the router are deleted.

You must configure the **parameter-map type inspect global** command before you configure the **per-box max-incomplete aggressive-aging** command.

Examples

The following example shows how to configure aggressive aging of half-opened sessions in a firewall session table:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# per-box max-incomplete 3456 aggressive-aging high 7890 low 5436
Router(config-profile)# end
```

Related Commands

Command	Description
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions for inspect parameter maps.
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

per-box tcp syn-flood limit

To configure the TCP synchronization (SYN) flood limit for each session listed in the firewall session table (the "box), use the **per-box tcp syn-flood limit** command in parameter-map type inspect configuration mode. To disable the TCP SYN flood limit configuration, use the **no** form of this command.

per-box tcp syn-flood limit *number*

no per-box tcp syn-flood limit *number*

Syntax Description

number	The number of half-opened connections that triggers TCP SYN cookie protection. Valid values are from 1 to 4294967295.

Command Default

The TCP SYN flood limit is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Per-box refers to the entire firewall session table.

TCP SYN-flooding attacks are a type of denial-of-service (DoS) attack. TCP SYN-flooding can take up all resources on a firewall or an end host, thereby causing denials of service to legitimate traffic. The Firewall TCP SYN Cookie feature protects the firewall from TCP SYN-flooding attacks. To prevent TCP SYN flooding on a firewall and the end hosts behind the firewall, configure the Firewall TCP SYN Cookie feature.

A half-opened session is a session that has not reached the established state.

You must configure the **parameter-map type inspect global** command before you configure the **per-box tcp syn-flood limit** command.

Examples

The following example shows how to configure the TCP SYN flood limit to 3400:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# per-box tcp syn-flood limit 3400
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

permit

To set conditions in named IP access list or object group access control list (OGACL) that will permit packets, use the **permit** command in the appropriate configuration mode. To remove a condition from an IP access list or an OGACL, use the **no** form of this command.

permit *protocol* [*source-addr source-wildcard*] {**any**| **host** {*address*| *name*}| **object-group** *object-group-name*} {*destination-addr destination-wildcard*| **any**| **host** {*address*| *name*}| **object-group** *object-group-name*} [**dscp** *dscp-value*| **precedence** *precedence-value*| **fragments** *fragment-value*| **option** *option-value*| **reflect** *access-list-name*| **time-range** *time-range-value*| **ttl** *match-value ttl-value* **[ttl-value]**| **tos** *tos-value*| **timeout** *max-time*| **log** [*log-value*]| **log-input** [*log-input-value*]]

no permit *protocol* [*source-addr source-wildcard*] {**any**| **host** {*address*| *name*}| **object-group** *object-group-name*} {*destination-addr destination-wildcard*| **any**| **host** {*address*| *name*}| **object-group** *object-group-name*}

permit {**tcp**| **udp**} {*source-addr source-wildcard*| **any**| **host** *source-addr*| **object-group** *source-obj-group*} {*destination-addr destination-wildcard*| **any**| **host** *dest-addr*| **object-group** *dest-obj-group*| *port-match-criteria* {*destination-addr destination-wildcard*| **any**| **host** *dest-addr*| **object-group** *dest-obj-group*}} [*port-match-criteria port-number*| **fragments**| **ack**| **established**| **fin**| **psh**| **rst**| **syn**| **urg**| **match-all** *match-value*| **match-any** *match-value*| **dscp** *dscp-value*| **precedence** *precedence-value*| **option** *option-value*| **time-range** *time-range-value*| **ttl** *match-value ttl-value* [*ttl-value*]| **tos** *tos-value*| **log** [*log-value*]| **log-input** [*log-input-value*]]

no permit {**tcp**| **udp**} {*source-addr source-wildcard*| **any**| **host** *source-addr*| **object-group** *source-obj-group*} {*destination-addr destination-wild-card*| **any**| **host** *dest-addr*| **object-group** *dest-obj-group*| *port-match-criteria* {*destination-addr destination-wild-card*| **any**| **host** *dest-addr*| **object-group** *dest-obj-group*}}

Syntax Description

protocol	Name or number of a protocol; valid values are; valid values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **object-group**, **tcp**, **pcp**, **pim**, **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
source-addr	(Optional) Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	(Optional) Wildcard bits to be applied to the source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.

any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address name*	Specifies the source or destination address and name of a single host.
object-group *object-group-name*	Specifies the source or destination name of the object group.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *dest-addr-group-name*	Specifies the destination address group name.
dscp *dscp-value*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the “Usage Guidelines” section for valid values.
precedence *precedence-value*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the “Usage Guidelines” section for a list of valid names.
fragments *fragment-value*	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List or OGACL Processing of Fragments" and “Fragments and Policy Routing” sections in the “Usage Guidelines” section.
option *option-value*	(Optional) Matches the packets with the given IP options value number; see the “Usage Guidelines” section for valid values.
reflect *access-list-name*	(Optional) Create reflexive access list entry.
time-range *time-range-value*	(Optional) Specifies a time-range entry name.
ttl *match-value ttl-value*	(Optional) Specifies the match packets with given TTL value; see the “Usage Guidelines” section for valid values.

tos *tos-value*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the "Usage Guidelines" section of the **access-list**(IP extended) command.
timeout *max-time*	Specifies the maximum time for a reflexive ACL to live; the valid values are from 1 to 2147483 seconds.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and port numbers and the user-defined cookie or router-generated hash value. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

log-value	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
log-input *log-input-value*	(Optional) Matches the log against this entry, including the input interface. After you specify the **log-input** keyword (and the associated *log-input-value* argument), you cannot specify any other keywords or settings for this command.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
object-group *source-obj-group*	Specifies the source address group name.
port-match-criteria port-number	Matches only packets on a given port number; see the “Usage Guidelines” section for valid values.

Command Default

There are no specific conditions under which a packet passes the access list.

Command Modes

Standard access-list configuration (config-std-nacl) Extended access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.4(22)T	The *word* argument was added to the **log** and **log-input** keywords.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

In Cisco IOS 15.0(1)M and later Releases, to remove the log entry from the **permit ip any any log** command, use the **permit ip any any** command.

In releases earlier than Cisco IOS Release15.0(1)M, to remove the **log** option from the **permit ip any any log** command, use the **no permit ip any any log** and the **permit ip any any** commands.

In Cisco IOS 15.0(1)M and later releases, to remove the log entry and the user-defined cookie, use the **permit ip any any** [*log-value*] command.

In releases earlier than Cisco IOS Release 15.0(1)M, to remove the log entry and user-defined cookies, use the **no permit ip any any log** [*log-value*] and **permit ip any any** commands.

Access List or OGACL Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in the table below:

Table 10: Access list or OGACL Processing of Fragments

If the Access-List Entry Has...	Then...

...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information:
	• The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.
	For an access list entry containing Layer 3 and Layer 4 information:
	• The entry is applied to nonfragmented packets and initial fragments:
	  • If the entry is a **permit**statement, the packet or fragment is permitted.
	  • If the entry is a **deny**statement, the packet or fragment is denied.
	• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and
	  • If the entry is a **permit**statement, the noninitial fragment is permitted.
	  • If the entry is a **deny** statement, the next access-list entry is processed.
	Note The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.

...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Ensure that you do not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent

fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The *source-addr* and *destination-addr*arguments allow you to create an object group based on a source or destination group. The following keywords and arguments are available:

- **dscp** *dscp-value* --(Optional) Matches the packets with the given DSCP value; the valid values are as follows:
  - **0** to **63**--Differentiated services codepoint value
  - **af11**--Matches the packets with AF11 dscp (001010)
  - **af12**--Matches the packets with AF12 dscp (001100)
  - **af13**--Matches the packets with AF13 dscp (001110)
  - **af21**--Matches the packets with AF21 dscp (010010)
  - **af22**--Matches the packets with AF22 dscp (010100)
  - **af23**--Matches the packets with AF23 dscp (010110)
  - **af31**--Matches the packets with AF31 dscp (011010)
  - **af32**--Matches the packets with AF32 dscp (011100)
  - **af33**--Matches the packets with AF33 dscp (011110)
  - **af41**--Matches the packets with AF41 dscp (100010)
  - **af42**--Matches the packets with AF42 dscp (100100)
  - **af43**--Matches the packets with AF43 dscp (100110)
  - **cs1**--Matches the packets with CS1 (precedence 1) dscp (001000)
  - **cs2**--Matches the packets with CS2 (precedence 2) dscp (010000)
  - **cs3**--Matches the packets with CS3 (precedence 3) dscp (011000)
  - **cs4**--Matches the packets with CS4 (precedence 4) dscp (100000)
  - **cs5**--Matches the packets with CS5 (precedence 5) dscp (101000)

  - **cs6**--Matches the packets with CS6 (precedence 6) dscp (110000)
  - **cs7**--Matches the packets with CS7 (precedence 7) dscp (111000)
  - **default**--Matches the packets with default dscp (000000)
  - **ef**--Matches the packets with EF dscp (101110)

- **fragments** --(Optional) Checks for noninitial fragments. See the table above.
- **log** --(Optional) Logs the matches against this entry.
- **log-input** --(Optional) Logs the matches against this entry, including the input interface.
- **option** *option-value* --(Optional) Matches the packets with given IP Options value. The valid values are as follows:
  - 0 to 255--IP Options value.
  - **add-ext**--Matches the packets with Address Extension Option (147).
  - **any-options**--Matches the packets with ANY Option.
  - **com-security**--Matches the packets with Commercial Security Option (134).
  - **dps**--Matches the packets with Dynamic Packet State Option (151).
  - **encode**--Matches the packets with Encode Option (15).
  - **eool**--Matches the packets with End of Options (0).
  - **ext-ip**--Matches the packets with Extended IP Option (145).
  - **ext-security**--Matches the packets with Extended Security Option (133).
  - **finn**--Matches the packets with Experimental Flow Control Option (205).
  - **imitd**--Matches the packets with IMI Traffic Desriptor Option (144).
  - **lsr**--Matches the packets with Loose Source Route Option (131).
  - **match-all**--Matches the packets if all specified flags are present.
  - **match-any**--Matches the packets if any specified flag is present.
  - **mtup**--Matches the packets with MTU Probe Option (11).
  - **mtur**--Matches the packets with MTU Reply Option (12).
  - **no-op**--Matches the packets with No Operation Option (1).
  - **psh**--Match the packets on the PSH bit.
  - **nsapa**--Matches the packets with NSAP Addresses Option (150).
  - **reflect**--Creates reflexive access list entry.
  - **record-route**--Matches the packets with Record Route Option (7).
  - **rst**--Matches the packets on the RST bit.
  - **router-alert**--Matches the packets with Router Alert Option (148).
  - **sdb**--Matches the packets with Selective Directed Broadcast Option (149).

- **security**--Matches the packets with Basic Security Option (130).
- **ssr**--Matches the packets with Strict Source Routing Option (137).
- **stream-id**--Matches the packets with Stream ID Option (136).
- **syn**--Matches the packets on the SYN bit.
- **timestamp**--Matches the packets with Time Stamp Option (68).
- **traceroute**--Matches the packets with Trace Route Option (82).
- **ump**--Matches the packets with Upstream Multicast Packet Option (152).
- **visa**--Matches the packets with Experimental Access Control Option (142).
- **zsu**--Matches the packets with Experimental Measurement Option (10).

- **precedence** *precedence-value* --(Optional) Matches the packets with given precedence value; the valid values are as follows:
  - 0 to 7--Precedence value.
  - **critical**--Matches the packets with critical precedence (5).
  - **flash**--Matches the packets with flash precedence (3).
  - **flash-override**--Matches the packets with flash override precedence (4).
  - **immediate**--Matches the packets with immediate precedence (2).
  - **internet**--Matches the packets with internetwork control precedence (6).
  - **network**--Matches the packets with network control precedence (7).
  - **priority**--Matches the packets with priority precedence (1).
  - **routine**--Matches the packets with routine precedence (0).
- **reflect acl-name** -- (Optional) Creates reflexive access list entry.
- **ttl** *match-value ttl-value* -- (Optional) Specifies the match packets with given TTL value; the valid values are as follows:
  - **eq**--Matches packets on a given TTL number.
  - **gt**--Matches packets with a greater TTL number.
  - **lt**--Matches packets with a lower TTL number.
  - **neq**--Matches packets not on a given TTL number.
  - **range**--Matches packets in the range of TTLs.
- **time-range** *time-range-value* --(Optional) Specifies a time-range entry name.
- **tos** --(Optional) Matches the packets with given ToS value; the valid values are as follows:
  - 0 to 15--Type of service value.
  - **max-reliability**--Matches the packets with the maximum reliable ToS (2).
  - **max-throughput**--Matches the packets with the maximum throughput ToS (4).

- **min-delay**--Matches the packets with the minimum delay ToS (8).
- **min-monetary-cost**--Matches the packets with the minimum monetary cost ToS (1).
- **normal**--Matches the packets with the normal ToS (0).

- **timeout** *max-time* -- (Optional) Specifies the maximum time for a reflexive ACL to live; the valid values are from 1 to 2147483 seconds.

Examples

The following example shows how to create an access list that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_network_object_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
```

The following example shows how to create an access list that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_network_object_group. In addition, logging is enabled for the access list, and all syslog entries for this ACE include the word MyServiceCookieValue:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any log MyServiceCookieValue
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

permit (Catalyst 6500 series switches)

To set conditions for a named IP access list, use the **permit** command in access-list configuration mode. To remove a condition from an access list, use the **no** form of this command.

permit *protocol* {*source-addr source-wildcard*| **addrgroup** *object-group-name*| **any**| **host** {*address*| *name*}} {*destination-addr destination-wildcard*| **addrgroup** *object-group-name*| **any**| **host** {*address*| *name*}}

permit {**tcp**| **udp**} {*source-addr source-wildcard*| **addrgroup** *source-addr-group-name*| **any**| **host** {**address**| **name**} *destination-addr destination-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {**address**| **name**}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*} {**addrgroup** *dest-addr-groupname*| *destination*| *destination-addr destination-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {**address**| **name**}| **lt** *port*| **neq** *port*| **portgroup** *destport-groupname*} [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **time-range** *time-range-name*| **tos** *tos*| **log [word]**| **log-input [word]**]

no permit *protocol* {*source-addr source-wildcard*| **addrgroup** *object-group-name*| **any**| **host** {*address*| *name*}} {*destination-addr destination-wildcard*| **addrgroup** *object-group-name*| **any**| **host** {*address*| *name*}}

no permit {**tcp**| **udp**} {*source-addr source-wildcard*| **addrgroup** *source-addr-group-name*| **any**| **host** {**address**| **name**} *destination-addr destination-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {**address**| **name**}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*} {**addrgroup** *dest-addr-groupname*| *destination*| *destination-addr destination-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {**address**| **name**}| **lt** *port*| **neq** *port*| **portgroup** *destport-groupname*} [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **time-range** *time-range-name*| **tos** *tos*| **log [word]**| **log-input [word]**]

Syntax Description

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
source-addr	Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	Wildcard bits to be applied to source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
addrgroup *object-group-name*	Specifies the source or destination name of the object group.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.

host *address*	Specifies the source or destination address of a single host.
host *name*	Specifies the source or destination name of a single host.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
addrgroup *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the “Usage Guidelines” section for valid values.
gt *port*	Matches only the packets with a greater port number; see the “Usage Guidelines” section for valid values.
lt *port*	Matches only the packets with a lower port number; see the “Usage Guidelines” section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the “Usage Guidelines” section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
addrgroup *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the “Usage Guidelines” section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the “Access List Processing of Fragments” and “Fragments and Policy Routing” sections in the “Usage Guidelines” section.

option *option*	(Optional) Matches the packets with the given IP options value number; see the “Usage Guidelines” section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the “Usage Guidelines” section for a list of valid names.
time-range *time-range-name*	(Optional) Specifies a time-range entry name.
tos *tos*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the “Usage Guidelines” section of the **access-list**(IP extended) command.
option option	(Optional) Matches packets with the IP options value; see the “Usage Guidelines” section for the valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the “Access List Processing of Fragments” and “Fragments and Policy Routing” sections in the “Usage Guidelines” section.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets, and if appropriate, the user-defined cookie or router-generated hash value. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers, and if appropriate, the user-defined cookie or router-generated hash value. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
log-input	(Optional) Matches the log against this entry, including the input interface. After you specify the **log-input** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

Command Default

There are no specific conditions under which a packet passes the named access list.

Command Modes

Access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.4(22)T	The *word* argument was added to the **log** and **log-input** keywords.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

The **portgroup** keyword appears only when you configure an extended access list.

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in the table below:

Table 11: Access list Processing of Fragments

If the Access-List Entry Has...	Then...

...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information:
	• The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.
	For an access list entry containing Layer 3 and Layer 4 information:
	• The entry is applied to nonfragmented packets and initial fragments:
	  • If the entry is a **permit**statement, the packet or fragment is permitted.
	  • If the entry is a **deny**statement, the packet or fragment is denied.
	• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and
	  • If the entry is a **permit**statement, the noninitial fragment is permitted.
	  • If the entry is a **deny** statement, the next access-list entry is processed.
	Note The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.

...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with

different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The **portgroup** *srcport-groupname or* **portgroup** *destport-groupname*keywords and arguments allow you to create an object group based on a source or destination group. The following keywords and arguments are available:

- **dscp** *value* --(Optional) Matches the packets with the given DSCP value; the valid values are as follows:
  - **0** to **63**--Differentiated services codepoint value
  - **af11**--Matches the packets with AF11 dscp (001010)
  - **af12**--Matches the packets with AF12 dscp (001100)
  - **af13**--Matches the packets with AF13 dscp (001110)
  - **af21**--Matches the packets with AF21 dscp (010010)
  - **af22**--Matches the packets with AF22 dscp (010100)
  - **af23**--Matches the packets with AF23 dscp (010110)
  - **af31**--Matches the packets with AF31 dscp (011010)
  - **af32**--Matches the packets with AF32 dscp (011100)
  - **af33**--Matches the packets with AF33 dscp (011110)
  - **af41**--Matches the packets with AF41 dscp (100010)
  - **af42**--Matches the packets with AF42 dscp (100100)
  - **af43**--Matches the packets with AF43 dscp (100110)
  - **cs1**--Matches the packets with CS1(precedence 1) dscp (001000)
  - **cs2**--Matches the packets with CS2(precedence 2) dscp (010000)
  - **cs3**--Matches the packets with CS3(precedence 3) dscp (011000)
  - **cs4**--Matches the packets with CS4(precedence 4) dscp (100000)
  - **cs5**--Matches the packets with CS5(precedence 5) dscp (101000)

- **cs6**--Matches the packets with CS6(precedence 6) dscp (110000)
- **cs7**--Matches the packets with CS7(precedence 7) dscp (111000)
- **default**--Matches the packets with default dscp (000000)
- **ef**--Matches the packets with EF dscp (101110)

- **fragments** --(Optional) Checks for noninitial fragments. See the table "Access List Processing of Fragments."
- **log** --(Optional) Logs the matches against this entry.
- **log-input** --(Optional) Logs the matches against this entry, including the input interface; the valid values are as follows:
- **option** *option* --(Optional) Matches the packets with given IP Options value. The valid values are as follows:
  - 0 to 255--IP Options value.
  - **add-ext**--Matches the packets with Address Extension Option (147).
  - **any-options**--Matches the packets with ANY Option.
  - **com-security**--Matches the packets with Commercial Security Option (134).
  - **dps**--Matches the packets with Dynamic Packet State Option (151).
  - **encode**--Matches the packets with Encode Option (15).
  - **eool**--Matches the packets with End of Options (0).
  - **ext-ip**--Matches the packets with Extended IP Option (145).
  - **ext-security**--Matches the packets with Extended Security Option (133).
  - **finn**--Matches the packets with Experimental Flow Control Option (205).
  - **imitd**--Matches the packets with IMI Traffic Desriptor Option (144).
  - **lsr**--Matches the packets with Loose Source Route Option (131).
  - **match-all**--Matches the packets if all specified flags are present.
  - **match-any**--Matches the packets if any specified flag is present.
  - **mtup**--Matches the packets with MTU Probe Option (11).
  - **mtur**--Matches the packets with MTU Reply Option (12).
  - **no-op**--Matches the packets with No Operation Option (1).
  - **psh**--Match the packets on the PSH bit.
  - **nsapa**--Matches the packets with NSAP Addresses Option (150).
  - **reflect**--Creates reflexive access list entry.
  - **record-route**--Matches the packets with Record Route Option (7).
  - **rst**--Matches the packets on the RST bit.
  - **router-alert**--Matches the packets with Router Alert Option (148).

- **sdb**--Matches the packets with Selective Directed Broadcast Option (149).
- **security**--Matches the packets with Basic Security Option (130).
- **ssr**--Matches the packets with Strict Source Routing Option (137).
- **stream-id**--Matches the packets with Stream ID Option (136).
- **syn**--Matches the packets on the SYN bit.
- **timestamp**--Matches the packets with Time Stamp Option (68).
- **traceroute**--Matches the packets with Trace Route Option (82).
- **ump**--Matches the packets with Upstream Multicast Packet Option (152).
- **visa**--Matches the packets with Experimental Access Control Option (142).
- **zsu**--Matches the packets with Experimental Measurement Option (10).

- **precedence** *value* --(Optional) Matches the packets with given precedence value; the valid values are as follows:
  - 0 to 7--Precedence value.
  - **critical**--Matches the packets with critical precedence (5).
  - **flash**--Matches the packets with flash precedence (3).
  - **flash-override**--Matches the packets with flash override precedence (4).
  - **immediate**--Matches the packets with immediate precedence (2).
  - **internet**--Matches the packets with internetwork control precedence (6).
  - **network**--Matches the packets with network control precedence (7).
  - **priority**--Matches the packets with priority precedence (1).
  - **routine**--Matches the packets with routine precedence (0).

- **reflect acl-name** [**timeout** *time*]-- (Optional) Creates reflexive access list entry. The timeout time keyword and argument specify the maximum time for a reflexive ACL to live; the valid values are from 1 to 2147483 seconds.
- **time-range** *name* --(Optional) Specifies a time-range entry name.
- **tos** --(Optional) Matches the packets with given ToS value; the valid values are as follows:
  - 0 to15--Type of service value.
  - **max-reliability**--Matches the packets with the maximum reliable ToS (2).
  - **max-throughput**--Matches the packets with the maximum throughput ToS (4).
  - **min-delay**--Matches the packets with the minimum delay ToS (8).
  - **min-monetary-cost**--Matches the packets with the minimum monetary cost ToS (1).
  - **normal**--Matches the packets with the normal ToS (0).

Examples

The following example shows how to create an access list that permits packets from the users in myAG if the protocol ports match the ports specified in myPG:

Router(config)# **ip access-list extended my-pbacl-policy**

Router(config-ext-nacl)# **permit tcp addrgroup myAG portgroup myPG any**

The following example shows how to create an access list that permits packets from the users in myAG if the protocol ports match the ports specified in myPG. The access list is log enabled, and the cookie value is set to myCookie:

Router(config)# **ip access-list extended my-pbacl-policy**

Router(config-ext-nacl)# **permit tcp addrgroup myAG portgroup myPG any log myCookie**

Related Commands

Command	Description
deny (Catalyst 6500 series switches)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
show ip access-lists	Displays the contents of all current IP access lists.

permit (IP)

To set conditions to allow a packet to pass a named IP access list, use the **permit** command in access list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

[*sequence-number*] **permit** *source* [*source-wildcard*]

[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

no *sequence-number*

no permit *source* [*source-wildcard*]

no permit *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

Internet Control Message Protocol (ICMP)

[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

Internet Group Management Protocol (IGMP)

[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

Transmission Control Protocol (TCP)

[sequence-number] permit tcp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any**| **match-all**} {+-} *flag-name*| **precedence** *precedence*| **tos** *tos*| **ttl** *operator value*| **log**| **time-range** *time-range-name*| **fragments**| **log** | [*user-defined-cookie*]]

User Datagram Protocol (UDP)

[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

Syntax Description

sequence-number	(Optional) Sequence number assigned to the permit statement. The sequence number causes the system to insert the statement in that numbered position in the access list.

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard*of 0.0.0.0 255.255.255.255. • Use **host** *source*as an abbreviation for a *source*and *source-wildcard*of *source*0.0.0.0.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source*as an abbreviation for a *source*and *source-wildcard*of *source*0.0.0.0.
protocol	Name or number of an Internet protocol. The *protocol* argument can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip**keyword. **Note** When the **icmp**, **igmp**, **tcp,** and **udp** keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the **permit** command. **Note** To configure a packet filter to allow BGP traffic, use protocol **tcp** and specify the port number as 179 or **bgp**

destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any**keyword as an abbreviation for the *destination*and *destination-wildcard*of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination*and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *destination*and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination*and *destination-wildcard* of *destination* 0.0.0.0.
option *option-name*	(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255, or by the corresponding IP Option name, as listed in the table in the “Usage Guidelines” section.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the “Usage Guidelines” section of the **access-list**(IP extended) command.

ttl *operator-value*	(Optional) Compares the TTL value in the packet to the TTL value specified in this **permit** statement. • The *operator* can be **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), or **range** (inclusive range). • The *value* can range from 0 to 255. • If the operator is **range**, specify two values separated by a space. • For Release 12.0S, if the operator is **eq** or **neq**, only one TTL value can be specified. • For all other releases, if the operator is **eq** or **neq**, as many as 10 TTL values can be specified, separated by a space.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.

user-defined-cookie	(Optional) User-defined cookie appended to the log message. The cookie: • Cannot be more than 64 characters. • Cannot start with hexadecimal notation (such as 0x). • Cannot be the same as, or a subset of, the following keywords: **fragment, reflect**, **time-range.** • Must contain alphanumeric characters only. The user-defined cookie is appended to the Allegro Crypto Engine (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.
icmp	Permits only ICMP packets. When you enter the **icmp** keyword, you must use the specific command syntax shown for the ICMP form of the **permit** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the "Usage Guidelines" section of the **access-list**(IP extended) command.
igmp	Permits only IGMP packets. When you enter the **igmp** keyword, you must use the specific command syntax shown for the IGMP form of the **permit** command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the "Usage Guidelines" section of the **access-list**(IP extended) command.
tcp	Permits only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **permit** command.

operator	(Optional) Compares source or destination ports. Operators are **eq** (equal) , **gt** (greater than),**lt** (less than), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port. The range operator requires two port numbers. Up to ten port numbers can be entered for the **eq** (equal) and **neq** (not equal) operators. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list (IP extended)** command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection.
match-any | **match-all**	(Optional) For the TCP protocol only: A match occurs if the TCP datagram has certain TCP flags set or not set. You use the **match-any**keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the **match-all**keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the **match-any**and **match-all**keywords with the **+**or **-**keyword and the *flag-name*argument to match on one or more TCP flags.
+ | **-** *flag-name*	(Optional) For the TCP protocol only: The **+** keyword matches IP packets if their TCP headers contain the TCP flags that are specified by the *flag-name* argument. The **-** keyword matches IP packets that do not contain the TCP flags specified by the *flag-name* argument. You must follow the **+** and **-** keywords with the *flag-name* argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.

udp	Permits only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **permit** command.

Command Default

There are no specific conditions under which a packet passes the named access list.

Command Modes

Access list configuration (config-ext-nacl)

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name*keyword and argument were added.
12.0(11)	The **fragments**keyword was added.
12.2(13)T	The igrp keyword was removed because the IGRP protocol was no longer available in Cisco IOS software.
12.2(14)S	The *sequence-number*argument was added.
12.2(15)T	The *sequence-number*argument was added.
12.3(4)T	The **option** *option-name* keyword and argument were added. The **match-any**, **match-all, +,**and **-**keywords and the *flag-name* argument were added.
12.3(7)T	Command functionality was modified to allow up to ten port numbers to be added after the **eq** and **neq** operators so that an access list entry can be created with noncontiguous ports.
12.4	The **drip** keyword was added to specify the TCP port number used for Optimized Edge Routing (OER) communication.
12.4(2)T	The **ttl** *operator value*keyword and arguments were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The *word* argument was added to the **log** keyword.
Cisco IOS XE Release 3.2	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **permit** command following the **ip access-list** command to define the conditions under which a packet passes the named access list.

Note In Cisco IOS XE, an inclusive port range for users to access a network cannot be matched in the extended ACL using the **permit** command.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **permit** statement is in effect.

log Keyword

A log message includes the access list number or access list name, and whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and port numbers, and the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute-interval). See the **ip access-list log-update** command for more information.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

If you enable Cisco Express Forwarding and then create an access list that uses the **log** keyword, the packets that match the access list are not Cisco Express Forwarding switched. They are fast-switched. Logging disables Cisco Express Forwarding .

Access List Filtering of IP Options

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from its URL: www.iana.org.

Cisco IOS software allows you to filter packets according to whether they contain one or more of the legitimate IP Options by entering either the IP Option value or the corresponding name for the *option-name* argument as shown in the table below.

Table 12: IP Option Values and Names

IP Option Value or Name	Description
0 to 255	IP Options values.
add-ext	Match packets with Address Extension Option (147).
any-options	Match packets with any IP Option.

IP Option Value or Name	Description
com-security	Match packets with Commercial Security Option (134).
dps	Match packets with Dynamic Packet State Option (151).
encode	Match packets with Encode Option (15).
eool	Match packets with End of Options (0).
ext-ip	Match packets with Extended IP Options (145).
ext-security	Match packets with Extended Security Option (133).
finn	Match packets with Experimental Flow Control Option (205).
imitd	Match packets with IMI Traffic Descriptor Option (144).
lsr	Match packets with Loose Source Route Option (131).
mtup	Match packets with MTU Probe Option (11).
mtur	Match packets with MTU Reply Option (12).
no-op	Match packets with No Operation Option (1).
nsapa	Match packets with NSAP Addresses Option (150).
psh	Match the packets on the PSH bit.
record-route	Match packets with Router Record Route Option (7).
reflect	Create reflexive access list entry.
router-alert	Match packets with Router Alert Option (148).
rst	Matche the packets on the RST bit.
sdb	Match packets with Selective Directed Broadcast Option (149).
security	Match packets with Base Security Option (130).
ssr	Match packets with Strict Source Routing Option (137).
stream-id	Match packets with Stream ID Option (136).

IP Option Value or Name	Description
syn	Matches the packets on the SYN bit.
timestamp	Match packets with Time Stamp Option (68).
traceroute	Match packets with Trace Route Option (82).
ump	Match packets with Upstream Multicast Packet Option (152).
visa	Match packets with Experimental Access Control Option (142).
zsu	Match packets with Experimental Measurement Option (10).

Filtering IP Packets Based on TCP Flags

The access list entries that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have very specific groups of TCP flags set or not set. Users can select any desired combination of TCP flags with which to filter TCP packets. Users can configure access list entries in order to allow matching on a flag that is set and on a flag that is not set. Use the **+** and **-** keywords with a flag name to specify that a match is made based on whether a TCP header flag has been set. Use the **match-any** and **match-all** keywords to allow the packet if any or all, respectively, of the flags specified by the **+** or **-** keyword and *flag-name* argument have been set or not set.

Permitting Optimized Edge Routing (OER) Communication

The **drip** keyword was introduced under the **tcp** keyword to support packet filtering in a network where OER is configured. The **drip** keyword specifies port 3949 that OER uses for internal communication. This option allows you to build a packet filter that permits communication between an OER master controller and border routers. The **drip** keyword is entered following the TCP source, destination addresses, and the **eq** operator. See the example in the “Examples” section.

Access List Processing of Fragments

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

If the Access-List Entry Has ...	Then ...

... no **fragments** keyword (the default behavior), and assuming all of the access list entry information matches,	For an access list entry that contains only Layer 3 information, the entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.
	For an access list entry that contains Layer 3 and Layer 4 information:
	• The entry is applied to nonfragmented packets and initial fragments.
	  • If the entry is a **permit**statement, then the packet or fragment is permitted.
	  • If the entry is a **deny**statement, then the packet or fragment is denied.
	• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and
	  • If the entry is a **permit**statement, then the noninitial fragment is permitted.
	  • If the entry is a **deny** statement, then the next access list entry is processed.
	Note The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.

... the **fragments** keyword, and assuming all of the access list entry information matches,	The access list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access list entry that contains any Layer 4 information.

Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases that involve access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list has entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy-routed, even if the first fragment is not policy-routed.

If you specify the **fragments** keyword in access list entries, a better match between the action taken for initial and noninitial fragments can be made, and it is more likely that policy routing will occur as intended.

Creating an Access List Entry with Noncontiguous Ports

For Cisco IOS Release 12.3(7)T and later releases, you can specify noncontiguous ports on the same access control entry, which greatly reduces the number of access list entries required for the same source address, destination address, and protocol. If you maintain large numbers of access list entries, we recommend that you consolidate them when possible by using noncontiguous ports. You can specify up to ten port numbers following the **eq** and **neq** operators.

Examples

The following example shows how to set conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.168.34.0  0.0.0.255
 permit 172.16.0.0  0.0.255.255
 permit 10.0.0.0  0.255.255.255
! (Note: all other access implicitly denied).
```

The following example shows how to permit Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet0
 ip access-group legal in
```

The following example shows how to set a permit condition for an extended access list named filter2. The access list entry specifies that a packet may pass the named access list only if it contains the NSAP Addresses IP Option, which is represented by the IP Option value nsapa.

```
ip access-list extended filter2
 permit ip any any option nsapa
```

The following example shows how to set a permit condition for an extended access list named kmdfilter1. The access list entry specifies that a packet can pass the named access list only if the RST IP flag has been set for that packet:

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst
```

The following example shows how to set a permit condition for an extended access list named kmdfilter1. The access list entry specifies that a packet can pass the named access list if the RST TCP flag or the FIN TCP flag has been set for that packet:

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst +fin
```

The following example shows how to verify the access list by using the **show access-lists** command and then to add an entry to an existing access list:

```
Router# show access-lists
Standard IP access list 1
2 permit 10.0.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.255.255
10 permit 10.0.0.0, wildcard bits 0.0.255.255
20 permit 10.0.0.0, wildcard bits 0.0.255.255
ip access-list standard 1
 15 permit 10.0.0.0 0.0.255.255
```

The following examples shows how to remove the entry with the sequence number of 20 from the access list:

```
ip access-list standard 1
 no 20
!Verify that the list has been removed.
Router# show access-lists
Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.4.0.0, wildcard bits 0.0.0.255
```

The following example shows how, if a user tries to enter an entry that is a duplicate of an entry already on the list, no changes occur. The entry that the user is trying to add is a duplicate of the entry already in the access list with a sequence number of 20.

```
Router# show access-lists 101
Extended IP access list 101
    10 permit ip host 10.0.0.0 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.0.0.0 host 10.2.54.2
    40 permit ip host 10.0.0.0 host 10.3.32.3 log
ip access-list extended 101
 100 permit icmp any any
Router# show access-lists 101
Extended IP access list 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

The following example shows what occurs if a user tries to enter a new entry with a sequence number of 20 when an entry with a sequence number of 20 is already in the list. An error message appears, and no change is made to the access list.

```
Router# show access-lists 101
Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
ip access-lists extended 101
 20 permit udp host 10.1.1.1 host 10.2.2.2
%Duplicate sequence number.
Router# show access-lists 101
Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

The following example shows several **permit** statements that can be consolidated into one access list entry with noncontiguous ports. The **show access-lists** command is entered to display a group of access list entries for the access list named aaa.

```
Router# show access-lists aaa
Extended IP access lists aaa
 10 permit tcp any eq telnet any eq 450
```

```
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

Because the entries are all for the same **permit** statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
ip access-list extended aaa
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
```

The following example shows the creation of the consolidated access list entry:

```
Router# show access-lists aaa
Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 450 679
```

The following access list filters IP packets containing Type of Service (ToS) level 3 with TTL values 10 and 20. It also filters IP packets with a TTL greater than 154 and applies that rule to noninitial fragments. It permits IP packets with a precedence level of flash and a TTL not equal to 1, and sends log messages about such packets to the console. All other packets are denied.

```
ip access-list extended canton
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
```

The following example shows how to configure a packet filter, for any TCP source and destination, that permits communication between an OER master controller and border router:

```
ip access-list extended 100
 permit any any tcp eq drip
 exit
```

The following example shows how to set a permit condition for an extended access list named filter_logging. The access list entry specifies that a packet may pass the named access list only if it is of TCP protocol type and destined to host 10.5.5.5, all other packets are denied. In addition, the logging mechanism is enabled and one of the user defined cookies (Permit_tcp_to_10.5.5.5 or Deny_all) is appended to the appropriate syslog entry.

```
ip access-list extended filter_logging
 permit tcp any host 10.5.5.5 log Permit_tcp_to_10.5.5.5
 deny ip any any log Deny_all
```

The following example shows how to configure a packet filter for any TCP source and destination that permits inbound and outbound BGP traffic:

```
ip access-list extended 100
 permit tcp any eq bgp any eq bgp
```

Related Commands

Command	Description
absolute	Specifies an absolute time when a time range is in effect.
access-list (IP extended)	Defines an extended IP access list.

Command	Description
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-group	Controls access to an interface.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
ip access-list resequence	Applies sequence numbers to the access list entries in an access list.
ip options	Drops or ignores IP Options packets that are sent to the router.
logging console	Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
show access-lists	Displays a group of access-list entries.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

permit *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

no permit *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol

permit icmp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]| *icmp-message*] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

permit tcp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] **[ack]** [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] **[established] [fin]** [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] **[psh]** [**range** {*port*| *protocol*}] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

permit udp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] [**range** {*port*| *protocol*}] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, **udp**, or **hbh**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.

source-ipv6-prefix/*prefix-length*	The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set permit conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with any protocol.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix*/*prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix*/*prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/ *prefix-length*	The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

host *destination-ipv6-address*	The destination IPv6 host address about which to set permit conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dest-option-type	(Optional) Matches IPv6 packets against the destination extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified. When this keyword is used, it also matches when the first fragment does not have Layer 4 information.
hbh	(Optional) Matches IPv6 packets against the hop-by-hop extension header within each IPv6 packet header.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(mobility) Matches IPv6 packets against the mobility extension header within each IPv6 packet header.
mobility-type	(Optional) Matches IPv6 packets against the mobility-type extension header within each IPv6 packet header. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Mobility header types. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error

reflect *name*	(Optional) Specifies a reflexive IPvi6 access list. Reflexive IPv6 access lists are created dynamically when an IPv6 packets matches a permit statement that contains the **reflect** keyword. The reflexive IPv6 access list mirrors the permit statement and times out automatically when no IPv6 packets match the permit statement. Reflexive IPv6 access lists can be applied to the TCP, UDP, SCTP, and ICMP for IPv6 packets.
timeout *value*	(Optional) Interval of idle time (in seconds) after which a reflexive IPv6 access list times out. The acceptable range is from 1 to 4294967295. The default is 180 seconds.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Matches IPv6 packets against the routing-type extension header within each IPv6 packet header. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.

icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the "Usage Guidelines" section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
{**range** *port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.

syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration (config-ipv6-acl)#

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.2(3)T	This command was modified. Support was added for the **hbh** keyword.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

The **permit** (IPv6) command is similar to the **permit** (IP) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix*/*prefix-length* and *destination-ipv6-prefix*/*prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit

- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Defining Reflexive Access Lists

To define an IPv6 reflexive list, a form of session filtering, use the **reflect** keyword in the **permit** (IPv6) command. The **reflect** keyword creates an IPv6 reflexive access list and triggers the creation of entries in the reflexive access list. The **reflect** keyword must be an entry (condition statement) in an IPv6 access list.

Note For IPv6 reflexive access lists to work, you must nest the reflexive access list using the **evaluate** command.

If you are configuring IPv6 reflexive access lists for an external interface, the IPv6 access list should be one that is applied to outbound traffic.

If you are configuring an IPv6 reflexive access list for an internal interface, the IPv6 access list should be one that is applied to inbound traffic.

IPv6 sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the IPv6 access list, the packet is also evaluated against the IPv6 reflexive permit entry.

As with all IPv6 access list entries, the order of entries is important, because they are evaluated in sequential order. When an IPv6 packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive permit entry, the packet will not be evaluated by the reflexive permit entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive permit entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive permit entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating that the packet belongs to a session in progress). The temporary entry specifies criteria that permit traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

The **permit** (IPv6) command with the **reflect** keyword enables the creation of temporary entries in the same IPv6 reflexive access list that was defined by the **permit** (IPv6) command. The temporary entries are created when an IPv6 packet exiting your network matches the protocol specified in the **permit** (IPv6) command. (The packet "triggers" the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a permit entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except that the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except that the port numbers are swapped.
- If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: The temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IPv6 traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IPv6 packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configured length of time (the timeout period), the entry will expire.

Examples

The following example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:ODB8:0300:0201::/64 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive access list named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network FEC0:0:0:0201::/64 (packets that have the site-local prefix FEC0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The third permit entry in the OUTBOUND list permits all ICMP packets to exit out of Ethernet interface 0.

The permit entry in the INBOUND list permits all ICMP packets to enter Ethernet interface 0. The **evaluate** command in the list applies the temporary IPv6 reflexive access list named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets. Refer to the **evaluate** command for more information on nesting IPv6 reflexive access lists within IPv6 ACLs.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any
ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT
interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

Note Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND access list, only TCP, UDP, and ICMP packets will be permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the access list denies all other packet types on the interface).

The following example shows how to allow the matching of any UDP traffic. The authentication header may be present.

```
permit udp any any sequence 10
```

The following example shows how to allow the matching of only TCP traffic if the authentication header is also present.

```
permit tcp any any auth sequence 20
```

The following example shows how to allow the matching of any IPv6 traffic where the authentication header is present.

```
permit ahp any any sequence 30
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

permit (MAC ACL)

To set conditions for a MAC access list, use the **permit** command in MAC access-list extended configuration mode. To remove a condition from an access list, use the **no** form of this command.

permit {*src_mac_mask*| **host name** *src_mac_name*| **any**} {*dest_mac_mask*| **host name** *dst_mac_name*| **any**} [{*protocol_keyword*| *ethertype_number ethertype_mask*} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

no permit {*src_mac_mask*| **host name** *src_mac_name*| **any**} {*dest_mac_mask*| **host name** *dst_mac_name*| **any**} [{*protocol_keyword*| *ethertype_number ethertype_mask*} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

Syntax Description

src_mac_mask	Specifies the MAC address mask that identifies a selected block of source MAC addresses. A value of 1 represents a wildcard in that position.
host name *src_mac_name*	Specifies a source host that has been named using the **mac host name** command.
any	Specifies any source or any destination host as an abbreviation for the *src_mac_mask*or *dest_mac_mask*value of 1111.1111.1111, which declares all digits to be wildcards .
dest_mac_mask	Specifies the MAC address mask that identifies a selected block of destination MAC addresses.
host name *dst_mac_name*	Specifies a destination host that has been named using the **mac host name** command.
protocol_keyword	(Optional) Specifies a named protocol (for example, ARP).
ethertype_number	(Optional) The EtherType number specifies the protocol within the Ethernet packet.
ethertype_mask	(Optional) The EtherType mask allows a range of EtherTypes to be specified together. This is a hexadecimal number from 0 to FFFF. An EtherType mask of 0 requires an exact match of the EtherType.
vlan *vlan_ID*	(Optional) Specifies a VLAN.
cos *cos_value*	(Optional) Specifies the Layer 2 priority level for packets. The range is from 0 to 7.

Command Default

This command has no defaults.

Command Modes

MAC access-list extended configuration (config-ext-macl)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

- The **vlan** and **cos** keywords are not supported in MAC ACLs used for VACL filtering.
- The **vlan** keyword for VLAN-based QoS filtering in MAC ACLs can be globally enabled or disabled and is disabled by default.
- Enter MAC addresses as three 2-byte values in dotted hexadecimal format. For example, 0123.4567.89ab.
- Enter MAC address masks as three 2-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- An entry without a protocol parameter matches any protocol.
- Enter an EtherType and an EtherType mask as hexadecimal values from 0 to FFFF.
- This list shows the EtherType values and their corresponding protocol keywords:
  - 0x0600--xns-idp--Xerox XNS IDP
  - 0x0BAD--vines-ip--Banyan VINES IP
  - 0x0baf--vines-echo--Banyan VINES Echo
  - 0x6000--etype-6000--DEC unassigned, experimental
  - 0x6001--mop-dump--DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
  - 0x6002--mop-console--DEC MOP Remote Console
  - 0x6003--decnet-iv--DEC DECnet Phase IV Route
  - 0x6004--lat--DEC Local Area Transport (LAT)
  - 0x6005--diagnostic--DEC DECnet Diagnostics
  - 0x6007--lavc-sca--DEC Local-Area VAX Cluster (LAVC), SCA
  - 0x6008--amber--DEC AMBER
  - 0x6009--mumps--DEC MUMPS
  - 0x0800--ip--Malformed, invalid, or deliberately corrupt IP frames
  - 0x8038--dec-spanning--DEC LANBridge Management

- 0x8039--dsm--DEC DSM/DDP
- 0x8040--netbios--DEC PATHWORKS DECnet NETBIOS Emulation
- 0x8041--msdos--DEC Local Area System Transport
- 0x8042--etype-8042--DEC unassigned
- 0x809B--appletalk--Kinetics EtherTalk (AppleTalk over Ethernet)
- 0x80F3--aarp--Kinetics AppleTalk Address Resolution Protocol (AARP)

Examples

This example shows how to create a MAC-Layer ACL named mac_layer that permits dec-phase-iv traffic with source address 0000.4700.0001 and destination address 0000.4700.0009, but denies all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# permit 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# deny any any
```

Related Commands

Command	Description
deny (MAC ACL)	Sets deny conditions for a named MAC access list.
mac access-list extended	Defines a MAC access list by name.
mac host	Assigns a name to a MAC address.
show mac access-group	Displays the contents of all current MAC access groups.

permit (reflexive)

To create a reflexive access list and to enable its temporary entries to be automatically generated, use the **permit**command in access-list configuration mode. To delete the reflexive access list (if only one protocol was defined) or to delete protocol entries from the reflexive access list (if multiple protocols are defined), use the **no** form of this command.

permit *protocol source source-wildcard destination destination-wildcard* **reflect** *name* [**timeout** *seconds*]

no permit *protocol source-wildcard destination destination-wildcard* **reflect** *name*

Syntax Description

protocol	Name or number of an IP protocol. It can be one of the keywords **gre**, **icmp**, **ip**, **ipinip**, **nos**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol, Transmission Control Protocol, and User Datagram Protocol), use the keyword **ip**.
source	Number of the network or host from which the packet is being sent. There are three other ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section “Usage Guidelines”). • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits (mask) to be applied to source. There are three other ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally not recommended (see the section “Usage Guidelines”). • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

destination	Number of the network or host to which the packet is being sent. There are three other ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally *not* recommended (see the section "Usage Guidelines"). • Use **host** *destination*as an abbreviation for a *destination* and *destination-wildcard* of destination 0.0.0.0.
destination- wildcard	Wildcard bits to be applied to the destination. There are three other ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. This keyword is normally *not* recommended (see the section "Usage Guidelines"). • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
reflect	Identifies this access list as a reflexive access list.
name	Specifies the name of the reflexive access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. The name can be up to 64 characters long.
timeout *seconds*	(Optional) Specifies the number of seconds to wait (when no session traffic is being detected) before entries expire in this reflexive access list. Use a positive integer from 0 to 232-1. If not specified, the number of seconds defaults to the global timeout value.

Command Default

If this command is not configured, no reflexive access lists will exist, and no session filtering will occur.

If this command is configured without specifying a **timeout** value, entries in this reflexive access list will expire after the global timeout period.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

For this command to work, you must also nest the reflexive access list using the **evaluate** command.

This command creates a reflexive access list and triggers the creation of entries in the same reflexive access list. This command must be an entry (condition statement) in an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to outbound traffic.

If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to inbound traffic.

IP sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the extended named IP access list, the packet is also evaluated against this reflexive **permit** entry.

As with all access list entries, the order of entries is important, because they are evaluated in sequential order. When an IP packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive **permit** entry, the packet will not be evaluated by the reflexive **permit** entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive **permit** entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive **permit** entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating the packet belongs to a session in progress). The temporary entry specifies criteria that permits traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

This command enables the creation of temporary entries in the same reflexive access list that was defined by this command. The temporary entries are created when a packet exiting your network matches the protocol specified in this command. (The packet "triggers" the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a **permit** entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except the port numbers are swapped.

If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: the temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).

- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IP traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IP packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configurable length of time (the timeout period), the entry will expire.

Examples

The following example defines a reflexive access list *tcptraffic*, in an outbound access list that permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic and denies all ICMP traffic. This example is for an external interface (an interface connecting to an external network).

First, the interface is defined and the access list is applied to the interface for outbound traffic.

```
interface Serial 1
 description Access to the Internet via this interface
 ip access-group outboundfilters out
```

Next, the outbound access list is defined and the reflexive access list *tcptraffic* is created with a reflexive **permit** entry.

```
ip access-list extended outboundfilters
 permit tcp any any reflect tcptraffic
```

Related Commands

Command	Description
evaluate	Nests a reflexive access list within an access list.
ip access-list	Defines an IP access list by name.

Command	Description
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.

permit (webvpn acl)

To set conditions to allow packets to pass a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list, use the **permit** command in webvpn acl configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit [**url** [**any**| *url-string*]] [**ip**| **tcp**| **udp**| **http**| **https**| **cifs**] [**any**| *source-ip source-mask*] [**any**| *destination-ip destination-mask*] **time-range** *time-range-name* **[syslog]**

no permit url [**any**| *url-string*] [**ip**| **tcp**| **udp**| **http**| **https**| **cifs**] [**any**| *source-ip source-mask*] [**any**| *destination-ip destination-mask*] **time-range** *time-range-name* **[syslog]**

Syntax Description

url	(Optional) Filtering rules are applied to a URL. • Use the **any** keyword as an abbreviation for any URL.
url-string	(Optional) URL string defined as follows: **scheme://host[:port][/path]** • **scheme** --Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string. • **host** --Can be a hostname or a host IP (host mask). The host can have one wildcard (*). • **port** --Can be any valid port number (1-65535). It is possible to have multiple port numbers separated by a comma (,). The port range is expressed using a dash (-). • **path** --Can be any valid path string. In the path string, the $user is translated to the current user name.
ip	(Optional) Permits only IP packets. When you enter the **ip** keyword, you must use the specific command syntax shown for the IP form of the **permit** command.
tcp	(Optional) Permits only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **permit** command.
udp	(Optional) Permitss only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **permit** command.

http	(Optional) Permits only HTTP packets. When you enter the **http** keyword, you must use the specific command syntax shown for the HTTP form of the **permit** command.
https	(Optional) Permits only HTTPS packets. When you enter the **https** keyword, you must use the specific command syntax shown for the HTTPS form of the **permit** command.
cifs	(Optional) Permits only CIFS packets. When you enter the **cifs**keyword, you must use the specific command syntax shown for the CIFS form of the **permit** command.
source-ip source-mask	(Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
destination-ip destination-mask	(Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
time-range *time-range-name*	Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
syslog	(Optional) System logging messages are generated.

Command Default

All packets are permitted.

Command Modes

Webvpn acl configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command following the **acl** command (in webvpn context configuration mode) to specify conditions under which a packet can pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this permit statement is in effect.

Examples

The following example shows that all packets from the URL “https://10.168.2.228:34,80-90,100-/public” are permitted to pass ACL “acl1”:

```
webvpn context context1
 acl acl1
  permit url “https://10.168.2.228:34,80-90,100-/public”
```

Related Commands

Command	Description
absolute	Specifies an absolute time for a time range.
deny (webvpn acl)	Sets conditions in a named SSL VPN access list that will deny packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Enables time-range configuration mode and defines time ranges for extended access lists.

pfs

To configure a server to notify the client of the central-site policy regarding whether PFS is required for any IP Security (IPsec) Security Association (SA), use the **pfs** command in global configuration mode or IKEv2 authorization policy configuration mode. To restore the default behavior, use the **no** form of this command.

pfs

no pfs

Syntax Description

This command has no arguments or keywords.

Command Default

The server will not notify the client of the central-site policy regarding whether PFS is required for any IPsec SA.

Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Before you use the **pfs** command, you must first configure the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command.

An example of an attribute-value (AV) pair for the PFS attribute is as follows:

```
ipsec:pfs=1
```

Examples

The following example shows that the server has been configured to notify the client of the central-site policy regarding whether PFS is required for any IPsec SA:

```
crypto ikev2 authorization policy
 pfs
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

pki-server

To specify the certificate server that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the Secure Device Provisioning (SDP) petitioner and the SDP registrar, use the **pki-server**command in tti-registrar configuration mode. To change the specified certificate server, use the **no** form of this command.

pki-server *label*

no pki-server *label*

Syntax Description

label	Name of certificate server.

Command Default

A certificate server is not associated with the TTI exchange; thus, the petitioner and registrar will not be able to communicate.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Although any device that contains a crypto image can be the registrar, it is recommended that the registrar be either a Cisco IOS certificate server registration authority (RA) or a Cisco IOS certificate server root.

Examples

The following example shows how to associate the certificate server “cs1” with the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
crypto wui tti registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.

pki trustpoint

To use the PKI trustpoints in the Rivest, Shamir and Adleman (RSA) signature authentication method, use the **pki trustpoint**command in IKEv2 profile configuration mode. To remove the trustpoint, use the **no** form of this command.

pki trust-point *trustpoint-name* [**sign**| **verify**]

no pki trust-point *trustpoint-name* [**sign**| **verify**]

Syntax Description

trustpoint-name	The trustpoint name as defined in the global configuration.
sign	(Optional) Uses certificates from the trustpoint to create a digital signature that is sent to the peer.
verify	(Optional) Uses certificates from the trustpoint to validate digital signatures received from thepeer.

Command Default

If there is no trustpoint defined in the IKEv2 profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

The **pki trustpoint** command specifies the trustpoints that are used with the RSA-signature authentication method. You can configure upto six truspoints.

Note If the **sign** or **verify** keyword is not specified, the trustpoint is used for signing and verification.

Examples

The following example specifies two trustpoints, trustpoint-local for local authentication using sign and trustpoint-remote for remote verification using verify:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# pki trustpoint trustpoint-local sign
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

police (zone policy)

To limit traffic matching within a firewall (inspect) policy, use the **police** command in policy-map class configuration mode. To remove traffic limiting from the firewall policy configuration , use the **no** form of this command.

police rate *bps* [**burst** *size*]

no police rate *bps* [**burst** *size*]

Syntax Description

rate *bps*	Specifies the average rate in bits per second (bps). Valid values are 8000 to 128000000000 (or 128 Gbps). **Note** Traffic limiting is in bps only; that is, packets per seconds (pps) and percent rates are not supported.
burst size	(Optional) Specifies the burst size in bytes. Valid values are 1000 to 2000000000 (2 Gb). The default normal burst size is 1500 bytes.

Command Default

Traffic limiting is disabled.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.0(1)SY	This command was modified. The maximum value for the *bps* and *size* arguments was increased.

Usage Guidelines

Issue the **police** command within an inspect policy to limit the number of concurrent connections allowed for applications such as Instant Messenger (IM) and peer-to-peer (P2P).

To effectively use the **police** command, you must also enable Cisco IOS stateful packet inspection within the inspect policy map. If you configure the **police** command without configuring the inspect action (via the **inspect** command), you will receive an error message and the **police** command will be rejected.

Because an inspect policy map can be applied only to a zone pair, and not an interface, the police action will be enforced on traffic that traverses the zone pair. (The direction is inherent to the specification of the zone pair.)

The police action is not allowed in policies that are attached to zone pairs involving a “self” zone. If you want to perform this task, you should use control plane policing.

Examples

The following example shows how to limit traffic matching with the inspect policy “p1”:

```
policy-map type inspect p1
 class type inspect c1
  inspect
  police rate 1000 burst 6100
```

The following example is sample output from the s**how policy-map type inspect zone-pair** command, which can now be used to verify the police action configuration:

```
Router# show policy-map type inspect zone-pair

Zone-pair: zp
Service-policy inspect : test-udp
  Class-map: check-udp (match-all)
   Match: protocol udp
   Inspect
    Packet inspection statistics [process switch:fast switch]
    udp packets: [3:4454]
    Session creations since subsystem startup or last reset 92

   Current session counts (estab/half-open/terminating) [5:33:0]
    Maxever session counts (estab/half-open/terminating) [5:59:0]
    Last session created 00:00:06
    Last statistic reset never
    Last session creation rate 61
    Last half-open session total 33
   Police
   rate 8000 bps,1000 limit
   conformed 2327 packets, 139620 bytes; actions: transmit
   exceeded 36601 packets, 2196060 bytes; actions: drop
   conformed 6000 bps, exceed 61000 bps
  Class-map: class-default (match-any)
   Match: any
   Drop (default action)
   0 packets, 0 bytes
```

Related Commands

Command	Description
show policy-map type inspect zone-pair	Displays the runtime inspect type policy map statistics and other information such as sessions existing on a specified zone pair.

policy

To define the Central Policy Push (CPP) firewall policy push, use the **policy** command in global configuration mode. To remove the CPP policy that was configured, use the **no** form of this command.

policy {**check-presence**| **central-policy-push access-list** {**in**| **out**} {*access-list-name*| *access-list-number*}}

no policy {**check-presence**| **central-policy-push access-list** {**in**| **out**} {*access-list-name*| *access-list-number*}}

Syntax Description

check-presence	Instructs the server to check for the presence of the specified firewall as shown as *firewall-type* on the client.
central-policy-push	Pushes the CPP firewall policy push. The configuration following this keyword specifies the actual policy, such as the input and output access lists that have to be applied by the client firewall of the type *firewall-type* .
access-list in	Defines the inbound access list on the virtual private network (VPN) remote client.
access-list out	Defines the outbound access list on the VPN remote client.
access-list-name | *access-list-number*	Access list name or number.

Command Default

The CPP policy is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Examples

The following example defines the CPP policy name as “hw-client-g-cpp.” The “Cisco-Security-Agent” policy type is mandatory. The CPP inbound list is “192” and the outbound list is “sample”:

```
crypto isakmp client firewall hw-client-g-cpp required Cisco-Security-Agent
```

```
 policy central-policy-push access-list in 192
 policy central-policy-push access-list out sample
```

policy check-presence:

The following example shows access lists that have been applied on a VPN remote client and later applied by the client firewall :

Examples

```
.
.
.
access-list 170 permit ip 172.18.124.0 0.0.0.255 any
access-list 170 permit ip 172.21.1.0 0.0.0.255 any
.
.
.
```

Examples

```
.
.
.
access-list 180 permit ip any 172.18.124.0 0.0.0.255
.
.
.
```

Inbound and outbound policies to be applied by the client firewall

```
.
.
.
crypto isakmp client firewall test required cisco-integrated-client-firewall
  policy central-policy-push access-list in 170
  policy central-policy-push access-list out 180
.
.
.
crypto isakmp client configuration group vpngroup1
  firewall policy test
.
.
.
```

Related Commands

Command	Description
crypto isakmp client firewall	Defines the CPP) firewall push policy on a server.

policy dynamic identity

To configure identity port mapping (IPM) to allow dynamic authorization policy download from an authorization server based on the identity of the peer, use the **policy dynamic identity** command in Cisco TrustSec manual configuration mode. Use the **no** form of the command to remove a policy.

policy dynamic identity *peer*

no policy dynamic identity *peer*

Syntax Description

peer	The peer device name or symbolic name in the authentication server's policy database associated with the policy to be applied to the peer.

Command Default

No policy is defined and traffic passes through without applying an SGT.

Command Modes

Cisco TrustSec manual configuration (config-if-cts-manual)

Command History

Release	Modification
12.2(50)SY	This command was introduced on the Catalyst 6500 Series Switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, no Cisco TrustSec encapsulation or encryption is performed.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the **policy static sgt** command is configured, the packet is tagged with the SGT configured in the policy static command.
  - If the **policy dynamic identity** command is configured, the packet is not tagged.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the **policy static sgt** command is configured without the trusted keyword, the SGT is replaced with the SGT configured in the policy static command.
  - If the **policy static sgt** command is configured with the trusted keyword, no change is made to the SGT.

- If the **policy dynamic identity** command is configured and the authorization policy downloaded from the authentication server indicates that the packet source is untrusted, the SGT is replaced with the SGT specified by the downloaded policy.
- If the**policy dynamic identity** command is configured and the downloaded policy indicates that the packet source is trusted, no change is made to the SGT.

Examples

```
Device(config-if-cts-manual)# policy dynamic identity my_peer_device_name
```

Related Commands

Command	Description
policy static sgt	Configures a static authorization policy for a Cisco TrustSec security group.

policy group

To enter webvpn group policy configuration mode to configure a group policy, use the **policy group** command in webvpn context configuration mode. To remove the policy group from the router configuration file, use the **no** form of this command.

policy group *name*

no policy group *name*

Syntax Description

name	Name of the policy group.

Command Default

Webvpn group policy configuration mode is not entered, and a policy group is not configured.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of end users. Entering the **policy group** command places the router in webvpn group policy configuration mode. After the group policy is configured, the policy group is attached to the SSL VPN context configuration by configuring the **default-group-policy** command.

Examples

The following example configures a policy group named ONE:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
```

Related Commands

Command	Description
banner	Configures a banner to be displayed after a successful login.

Command	Description
citrix enabled	Enables Citrix application support for end users in a policy group.
default-group-policy	Configures a default group policy for SSL VPN sessions.
filter citrix	Configures a Citrix application access filter.
filter tunnel	Configures a SSL VPN tunnel access filter.
functions	Enables a file access function or tunnel mode support in a group policy configuration.
hide-url-bar	Prevents the URL bar from being displayed on the SSL VPN portal page.
nbns-list (policy group)	Attaches a NBNS server list to a policy group configuration.
port-forward (policy group)	Attaches a port-forwarding list to a policy group configuration.
svc address-pool	Configures a pool of IP addresses to assign to end users in a policy group.
svc default-domain	Configures the domain for a policy group.
svc dns-server	Configures DNS servers for policy group end users.
svc dpd-interval	Configures the DPD timer value for the gateway or client.
svc homepage	Configures the URL of the web page that is displayed upon successful user login.
svc keep-client-installed	Configures the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled.
svc msie-proxy	Configures MSIE browser proxy settings for policy group end users.
svc msie-proxy server	Specifies a Microsoft Internet Explorer proxy server for policy group end users.
svc rekey	Configures the time and method that a tunnel key is refreshed for policy group end users.
svc split	Configures split tunneling for policy group end users.

Command	Description
svc wins-server	Configures configure WINS servers for policy group end users.
timeout	Configures the length of time that an end user session can remain idle or the total length of time that the session can remain connected.
url-list (policy group)	Attaches a URL list to policy group configuration.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

policy static sgt

To configure a static authorization policy for a Cisco TrustSec security group, use the **policy static sgt** command in Cisco TrustSec manual configuration mode. Use the **no** form of the command to remove a policy.

policy static sgt *tag* [**trusted**]

no policy static sgt *tag* [**trusted**]

Syntax Description

tag	Specifies the SGT in decimal format. The range is 1 to 65533.
trusted	Optional. Indicates that ingress traffic on the interface with this SGT should not have its tag overwritten.

Command Default

No static policy is defined.

Command Modes

Cisco TrustSec manual configuration (config-if-cts-manual)

Command History

Release	Modification
12.2(50)SY	This command was introduced on the Catalyst 6500 Series Switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.
Cisco IOS XE Release 3.9S	This command was modified. Support was added for the Cisco ASR 1000 Series Routers.

Usage Guidelines

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, no Cisco TrustSec encapsulation or encryption is performed.
- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the **policy static sgt** command is configured, the packet is tagged with the SGT configured in the policy static command.
  - If the **policy dynamic identity** command is configured, the packet is not tagged.

- If the selected SAP mode allows SGT insertion and an incoming packet carries an SGT, the tagging policy is as follows:
  - If the **policy static sgt** command is configured without the **trusted** keyword, the SGT is replaced with the SGT configured in the policy static command.
  - If the **policy static sgt** command is configured with the **trusted** keyword, no change is made to the SGT.
  - If the **policy dynamic identity** command is configured and the authorization policy downloaded from the authentication server indicates that the packet source is untrusted, the SGT is replaced with the SGT specified by the downloaded policy.
  - If the **policy dynamic identity** command is configured and the downloaded policy indicates that the packet source is trusted, no change is made to the SGT.

If the **policy static sgt** command is not configured, traffic may be tagged according to IP-SGT bindings specified by the **cts role-based sgt-map interface** command or learned from SXP. Traffic may also pass through without applying an SGT if no IP-SGT binding is found.

Note SAP is not supported on Cisco ASR 1000 Series Routers.

Examples

```
Device(config-if-cts-manual)# policy static sgt 7 trusted
```

Related Commands

Command	Description
policy dynamic identity	Configures identity port mapping (IPM) to allow dynamic authorization policy download from an authorization server based on the identity of the peer.
cts role-based sgt-map interface	Manually maps a source IP address to an SGT on either a host or a VRF.

policy-map type control mitigation

To configure a mitigation type policy map for Transitory Messaging Services (TMS), use the **policy-map type control mitigation** command in global configuration mode. To remove the policy map from the router configuration file, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **policy-map type control mitigation** command is not available in Cisco IOS software.

policy-map type control mitigation *name*

no policy-map type control mitigation *name*

Syntax Description

name	Name of the mitigation type policy map.

Command Default

A mitigation type policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The mitigation type policy map is used to configure a mitigation type service policy (TMS Rules Engine configuration). The mitigation type policy map is configured on only the consumer. Entering the **policy-map type control mitigation** command places the router in policy-map configuration mode.

The mitigation type policy map is configured to bind mitigation type class and parameter maps together, creating a mitigation type service policy. The mitigation type class map is configured to match a class of traffic to a primitive and priority level. The mitigation type parameter map is configured to set the next-hop variable for a redirect mitigation enforcement action.

Attaching the Policy Map to the Global TMS process

The mitigation type service policy is activated by attaching the mitigation type policy map to the TMS type policy map in policy-map class configuration mode. The TMS type policy map is then attached to the global consumer configuration by configuring the **service-policy** command in consumer configuration mode.

Examples

Examples

The following example configures the Rules Engine to send priority 5 redirect threat mitigation traffic to a null interface (black hole):

```
Router(config)# parameter-map type mitigation MIT_PAR_1

Router(config-profile)# variable RTBH NULL0
Router(config-profile)# exit
Router(config)# class-map type control mitigation match-all MIT_CLASS_1
Router(config-cmap)# match priority 5
Router(config-cmap)# match primitive redirect
Router(config-cmap)# exit
Router(config)# policy-map type control mitigation MIT_POL_1
Router(config-pmap)# class MIT_CLASS_1
Router(config-pmap-c)# redirect route $RTBH
Router(config-pmap-c)# end
```

Examples

The following example creates a Rules Engine configuration and activates it under the global consumer process:

```
Router(config)# class-map type control mitigation match-all MIT_CLASS_2

Router(config-cmap)# match primitive block

Router(config-cmap)# match priority 1

Router(config-cmap)# exit
Router(config)# parameter-map type mitigation MIT_PAR_2
Router(config-profile)# variable COLLECTION ipv4 192.168.1.1
Router(config-profile)# exit
Router(config)# policy-map type control mitigation MIT_POL_2
Router(config-pmap)# class MIT_CLASS_2
Router(config-pmap-c)# redirect route
Router(config-pmap-c)# source parameter MIT_PAR_2
Router(config-pmap-c)# exit

Router(config-pmap)# exit

Router(config)# policy-map type control tms TMS_POL_1

Router(config-pmap)# class TMS_CLASS_1

Router(config-pmap-c)# mitigation TMS_PAR_1
Router(config-pmap-c)# service-policy MIT_POL_2

Router(config-pmap-c)# exit

Router(config-pmap)# exit

Router(config)# tms consumer

Router(config-cons)# service-policy type tms TMS_POL_1
Router(config-cons)# end
```

Related Commands

Command	Description
acl drop	Configures an ACL drop enforcement action in a TMS Rules Engine configuration.

Command	Description
class-map type control mitigation	Configures a mitigation type class map.
ignore (TMS)	Configures the TMS Rules Engine to ignore a mitigation enforcement action.
match primitive	Configures a primitive match in a mitigation type class map.
match priority	Configures the match priority level for a mitigation enforcement action.
parameter-map type mitigation	Configures a mitigation type parameter map.
redirect route	Configures a redirect enforcement action in a mitigation type policy map.
service-policy (class-map)	Attaches a policy map to a class.
service-policy type tms	Binds a TMS type service policy to a global consumer process.
source parameter	Attaches a mitigation type parameter map to a policy-map class configuration.
tms-class	Associates an interface with an ACL drop enforcement action.
variable	Defines the next-hop variable in a mitigation type parameter map.

policy-map type control tms

To configure a Transitory Messaging Services (TMS) type policy map, use the **policy-map type control tms** command in global configuration mode. To remove the policy map from the router configuration file, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **policy-map type control tms** command is not available in Cisco IOS software.

policy-map type control tms *name*

no policy-map type control tms *name*

Syntax Description

name	The name of the TMS type policy map.

Command Default

A TMS type policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The TMS type policy map is configured on the consumer. Entering the **policy-map type control tms** command places the router in policy-map configuration mode.

The TMS type policy map is configured to bind (or attach) TMS protocol configuration and TMS group members (routers and networking devices) to the global consumer process. The TMS type class map defines the TMS group or groups over which TMS is deployed. The TMS type parameter map defines TMS protocol specific parameters, such as operational timers and event logging.

Attaching the Policy Map to the Global TMS process

TMS type class and parameter maps are attached to the policy map to create a TMS type service policy. It is activated by configuring the **service-policy type tms** command under the global consumer process.

Note The mitigation type service policy (TMS Rules Engine configuration) is activated by attaching the mitigation type policy map to the TMS type policy map in policy-map class configuration mode. The TMS type policy map is then attached to the global consumer configuration.

Examples

Examples

The following example configures a TMS type service policy and a mitigation type service policy (TMS Rules configuration) on a consumer:

```
Router(config)# class-map type control tms TMS_CLASS_1

Router(config-cmap)# match tidp-group 10
Router(config-cmap)# exit

Router(config)# class-map type control mitigation match-all MIT_CLASS_2

Router(config-cmap)# match primitive block

Router(config-cmap)# match priority 1

Router(config-cmap)# exit

Router(config)# parameter-map type tms TMS_PAR_1

Router(config-profile)# controller ipv4 10.1.1.1

Router(config-profile)# logging tms events

Router(config-profile)# registration retry interval 60
Router(config-profile)# registration retry count 5
Router(config-profile)# exit

Router(config)# parameter-map type mitigation MIT_PAR_2

Router(config-profile)# variable COLLECTION ipv4 192.168.1.1

Router(config-profile)# exit

Router(config)# policy-map type control mitigation MIT_POL_2

Router(config-pmap)# class MIT_CLASS_2

Router(config-pmap-c)# redirect route

Router(config-pmap-c)# source parameter MIT_PAR_2
Router(config-pmap-c)# exit

Router(config-pmap)# exit

Router(config)# policy-map type control tms TMS_POL_1

Router(config-pmap)# class TMS_CLASS_1

Router(config-pmap-c)# mitigation TMS_PAR_1

Router(config-pmap-c)# service-policy MIT_POL_2

Router(config-pmap-c)# exit

Router(config-pmap)# exit
Router(config)# tms consumer
Router(config-cons)# service-policy type tms TMS_POL_1
```

```
Router(config-cons)# end
```

Related Commands

Command	Description
class-map type control mitigation	Configures a mitigation type class map.
class-map type control tms	Configures a TMS type class map.
parameter-map type mitigation	Configures a mitigation type parameter map.
parameter-map type tms	Configures a TMS type parameter map.
policy-map type control mitigation	Configures a mitigation type policy map.
service-policy (class-map)	Attaches a policy map to a class.
service-policy type tms	Binds a TMS type service policy to a global consumer process.
tms consumer	Configures a consumer process on a router or networking device.
tms controller	Configures a controller process on a router or networking device.

policy-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map, use the **policy-map type inspect** command in global configuration mode. To delete an inspect-type policy map, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Policy Map Syntax

policy-map type inspect *policy-map-name*

no policy-map type inspect *policy-map-name*

Layer 7 (Application-Specific) Policy Map Syntax

policy-map type inspect *protocol-name policy-map-name*

no policy-map type inspect *protocol-name policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

protocol-name	Layer 7 application-specific policy map. The supported protocols are as follows:
	• **gtpv0 —**General Packet Radio Service (GPRS) Tunnel Protocol Version 0 (GTPv0).
	• **gtpv1—**GTP Version 1 (GTPv1)
	• **h323 —**H.323 protocol, Version 4
	• **http —**HTTP
	• **im —**Instant Messenger (IM) protocol. For IM, the supported IM protocols include:
	  • AOL Version 5 and later versions
	  • I Seek You (ICQ) Version 2003b.5.56.1.3916.85
	  • MSN Messenger Version 6.x and 7.x
	  • Windows Messenger Version 5.1.0701
	  • Yahoo Messenger Version 9.0 and later versions
	• **imap —**Internet Message Access Protocol (IMAP)
	• **p2p —**Peer-to-peer (P2P) protocol
	• **pop3 —**Post Office Protocol, Version 3 (POP3)
	• **sip —**Session Initiation Protocol (SIP)
	• **smtp —**Simple Mail Transfer Protocol (SMTP)
	• **sunrpc —**Sun Remote Procedure Call (SUNRPC)

Command Default

No policy map is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Release	Modification
12.4(9)T	This command was modified. Support for the following protocols and keywords was added: • P2P protocol and the **p2p** keyword • IM protocol and the **im** keyword
12.4(15)XZ	This command was modified. Support for SIP was added.
12.4(20)T	This command was modified. Support was added for the ICQ and Windows Messenger IM protocols, and following keywords were added: **icq**, **winmsgr**. Support was added for the H.323 VoIP protocol and the following keyword was added: **h323**.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.4S	This command was modified. The following GTP keywords were added: **gtpv0**, **gtpv1**.

Usage Guidelines

Use the **policy-map type inspect** command to create a Layer 3 and Layer 4 inspect-type policy map or a Layer 7 application-specific inspect-type policy map. After you create a policy map, you should enter the **class type inspect** command (as appropriate for your configuration) to specify the traffic (class) on which an action is to be performed. The class was previously defined in a class map. Thereafter, you should enter the **inspect** command to enable Cisco IOS stateful packet inspection and to specify inspect-specific parameters in a parameter map.

Layer 3, Layer 4 (Top Level) Policy Maps

Top-level policy maps allow you to define high-level actions such as **inspect**, **drop**, **pass**, and **urlfilter**. You can attach the maps to a target (zone pair). The maps can contain “child” policies that are also known as application-specific Layer 7 policies.

Layer 7 (Application-Specific) Policy Maps

Application-specific policy maps are used to specify a policy for an application protocol. For example, if you want to drop HTTP traffic with Uniform Resource Identifier (URI) lengths exceeding 256 bytes, you must configure an HTTP policy map to do that. Application-specific policy maps cannot be attached directly to a target (zone pair). They must be configured as “child” policies in a top-level Layer 3 or Layer 4 policy map.

The following protocols are supported for Cisco IOS XE Release 3.4S.

- GTPv0
- GTPv1
- HTTP
- IMAP
- Match-all Logical-AND all matching statements under this classmap
- Match-any Logical-OR all matching statements under this classmap

- POP3
- SMTP
- Sun RPC

Examples

The following example shows how to specify the traffic class (host) on which the drop action is to be performed:

```
policy-map type inspect mypolicy
 class type inspect host
 drop
```

The following example shows how to configure a policy map named my-im-pmap policy map with two IM classes, AOL and Yahoo Messenger, and allow only text-chat messages to pass through. When any packet with a service other than text-chat is seen, the connection will be reset.

```
class-map type inspect aol match-any my-aol-cmap
 match service text-chat
!
class-map type inspect ymsgr match-any my-ysmgr-cmap
 match service any
!
policy-map type inspect im my-im-pmap
 class type inspect aol my-aol-cmap
 allow
 log
!
 class type inspect ymsgr my-ysmgr-cmap
 reset
 log
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.

policy-map type inspect urlfilter

To create or modify a URL filter type inspect policy map, use the **policy-map type inspect urlfilter** command in global configuration mode. To delete a URL filter type inspect policy map, use the **no** form of this command.

policy-map type inspect urlfilter *policy-map-name*

no policy-map type inspect urlfilter *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy map is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **policy-map type inspect urlfilter**command to create a URL filter type inspect policy map. The policy map specifies the traffic (**class type urlfilter**) and the actions to be performed on that traffic for the specified URL filtering policy.

Before you create a URL filter type inspect policy map, use the following commands:

- **class-map type urlfilter** command to configure the match criteria for the traffic.
- **parameter-map type urlfpolicy** command to specify the parameters for the URL filtering server. If you are configuring a policy for a Trend Router Provisioning Server (TRPS), you must also specify the global filtering parameters with the **parameter-map type trend-global** command.

After you create a policy map, use the following commands to configure the URL filtering policy:

- **class type urlfilter [trend | n2h2 | websense**] *class-name*-- Specifies the class of traffic to which the policy applies. If you specify an optional URL filtering server, you must also use the **parameter type urlfpolicy** command to specify the appropriate per-policy parameters for that URL filtering server.

For each class, use one of the URL filtering action commands to specify how to handle a URL that matches the class map. The table below lists the URL filtering action commands.

Table 13: URL Filtering Action Commands

Command	Description
allow	Permits access to the requested URL.
log	Logs the URL request.
reset	Resets the HTTP connection at both ends.
server-specified action	Specifies that the traffic is handled by the URL filtering server. This action is valid only for Websense and N2H2 classes.

- **description** *string* --Describes the policy.
- **exit** --Exits the policy map.
- **no** --Negates or sets the default value for a command.
- **parameter type urlfpolicy [trend | n2h2 | websense**]--Specifies what type of URL filtering this policy applies to: local (default), Trend Micro, SmartFilter, or Websense.
- **rename** *policy-map-name* --Specifies a new name for the policy map.

Examples

The following example shows a how to create a URL filter type inspect policy for a Trend Micro URL filtering server. The policy logs URL requests that match the URL categories specified in the class drop-category, and then resets the connection, thus denying the request.

```
class-map type urlfilter trend match-any drop-category
 match url category Gambling
 match url category Personals-Dating
parameter-map type trend-global global-parameter-map
 server trend.example.com
parameter-map type urlfpolicy trend g1-trend-pm
 max-request 2147483647
 max-resp-pak 20000
 allow-mode on
 truncate hostname
 block-page message "group1: 10.10.10.0 is blocked by Trend."
policy-map type inspect urlfilter g1-trend-policy
 parameter type urlfpolicy trend g1-trend-parameter-map
 class type urlfilter trend drop-category
  log
 reset
```

The following example shows a filtering policy for a Websense URL filtering server. The policy logs and allows URL requests that are in the trusted domain class, logs and denies URL requests that are in the untrusted domain class, and logs and denies URL requests that are in the keyword class.

```
policy-map type inspect urlfilter websense-policy
 parameter type urlfpolicy websense websense-parameter-map
 class type urlfilter trusted-domain-class
  log
  allow
 class type urlfilter untrusted-domain-class
  log
  reset
```

```
class type urlfilter keyword-class
 log
 reset
```

Related Commands

Command	Description
class-map type urlfilter	Specifies the class on which a policy action is to be performed.
class type urlfilter	Associates a URL filter class map with a URL filtering policy maps.
parameter-map type trend-global	Creates or modifies the parameter map for global TRPS parameters.
parameter-map type urlfpolicy	Creates or modifies a parameter map for a URL filtering policy.

pool (isakmp-group)

To define a local pool address, use the **pool** command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To remove a local pool from your configuration, use the **no** form of this command.

[**ipv6**] **pool** *name*

no [**ipv6**] **pool** *name*

Syntax Description

ipv6	(Optional) Specifies an IPv6 address pool. To specify an IPv4 address, execute the command without this keyword.
name	Name of the local address pool.

Command Default

No local pool address is defined.

Command Modes

ISAKMP group configuration (config-isakmp-group)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

Use the pool command to refer to an IP local pool address, which defines a range of addresses that will be used to allocate an internal IP address to a client. Although a user must define at least one pool name, a separate pool may be defined for each group policy.

Note This command must be defined and refer to a valid IP local pool address, or the client connection will fail.

You must enable the following commands before enabling the **dns** command:

- **crypto isakmp client configuration group** --Specifies the group policy information that has to be defined or changed.
- **crypto ikev2 authorization policy** --Specifies the local group policy authorization parameters.

Examples

The following example shows how to refer to the local pool address named dog:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
!
ip local pool dog 10.1.1.1 10.1.1.254
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

port

To specify the port on which a device listens for RADIUS requests from configured RADIUS clients, use the **port** command in dynamic authorization local server configuration mode. To restore the default, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Port number. The default value is port 1700.

Command Default

The device listens for RADIUS requests on the default port (port 1700).

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **port** command to specify the ports on which the router will listen for requests from RADIUS clients.

Examples

The following example specifies port 1650 as the port on which the device listens for RADIUS requests:

```
aaa server radius dynamic-author
 client 10.0.0.1
 port 1650
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

port (IKEv2 cluster)

To define the port number to be used by a Internet Key Exchange Version 2 (IKEv2) cluster to connect to the master gateway in a Hot Standby Router Protocol (HSRP) group, use the **port** command in IKEv2 cluster configuration mode. To revert to the default port, use the **no** form of this command.

port *port-number*

no port

Syntax Description

port-number	Port number used by an IKEv2 cluster. The range is from 1 to 65535. The default is 2012.

Command Default

No port number is defined.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **port** command.

Examples

In the following example, the IKEv2 CLB slaves connect to the CLB Master using the port number 2221:

```
Router(config)# crypto ikev2 cluster
Router(config-ikev2-cluster)# port 2221
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

port (TACACS+)

To specify the TCP port to be used for TACACS+ connections, use the **port**command in TACACS+ server configuration mode. To remove the TCP port, use the **no** form of this command.

port [*number*]

no port [*number*]

Syntax Description

number	(Optional) Specifies the port where the TACACS+ server receives access-request packets. The range is from 1 to 65535.

Command Default

If no port is configured, port 49 is used.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

TCP port 49 is used if the *number* argument is not used when using the **port** command.

Examples

The following example shows how to specify TCP port 12:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

port-forward

To enter webvpn port-forward list configuration mode to configure a port-forwarding list, use the **port-forward** command in webvpn context configuration mode. To remove the port-forwarding list from the SSL VPN context configuration, use the **no** form of this command.

port-forward *name*

no port-forward *name*

Syntax Description

name	Name of the port-forwarding list.

Command Default

Webvpn port-forward list configuration mode is not entered, and a port-forwarding list is not configured.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **port-forward** command is used to create the port-forwarding list. Application port number mapping (port forwarding) is configured with the **local-port** command in webvpn port-forward configuration mode.

A port-forwarding list is configured for thin client mode SSL VPN. Port forwarding extends the cryptographic functions of the SSL-protected browser to provide remote access to TCP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the SSL VPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the SSL VPN session.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# port-forward EMAIL

Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port
 110 description POP3

Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com remote-port
 25 description SMTP

Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com remote-port
 143 description IMAP
```

Related Commands

Command	Description
local-port (WebVPN)	Remaps an application port number in a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

port-forward (policy group)

To attach a port-forwarding list to a policy group configuration, use the **port-forward**command in webvpn group policy configuration mode. To remove the port-forwarding list from the policy group configuration, use the **no** form of this command.

port-forward *name* [**auto-download** [**http-proxy** [**proxy-url** *homepage-url*]]| **http-proxy** [**proxy-url** *homepage-url*] **[auto-download]**]

no port-forward *name* [**auto-download** [**http-proxy** [**proxy-url** *homepage-url*]]| **http-proxy** [**proxy-url** *homepage-url*] **[auto-download]**]

Syntax Description

name	Name of the port-forwarding list that was configured in webvpn context configuration mode.
auto-download	(Optional) Allows for automatic download of the port-forwarding Java applet on the portal page of a website.
http-proxy	(Optional) Allows the Java applet to act as a proxy for the browser of the user.
proxy-url *homepage-url*	(Optional) Page at this URL address opens as the portal page of the user.

Command Default

A port-forwarding list is not attached to a policy group configuration.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The **auto-download** keyword was added.

Usage Guidelines

The configuration of this command applies to only clientless access mode. In clientless mode, the remote user accesses the internal or corporate network using the web browser on the client machine.

Examples

The following example shows how to apply the port-forwarding list to the policy group configuration:

```
webvpn context context1
```

```
 port-forward EMAIL
  local-port 30016 remote-server mail.company.com remote-port 110 description POP3
  local-port 30017 remote-server mail.company.com remote-port 25 description SMTP
  local-port 30018 remote-server mail.company.com remote-port 143 description IMAP
  exit
 policy group ONE
 port-forward EMAIL auto-download
```

The following example shows that HTTP proxy has been configured. The page at URL "http://www.example.com" will automatically download as the home page of the user.

```
webvpn context myContext
 ssl authenticate verify all
 !
 !
 port-forward "email"
   local-port 20016 remote-server "ssl-server1.sslvpn-ios.com" remote-port 110 description
 "POP-ssl-server1"
 !
 policy group myPolicy
   port-forward "email" auto-download http-proxy proxy-url "http://www.example.com"
 inservice
```

Related Commands

Command	Description
local-port (WebVPN)	Remaps an application port number in a port-forwarding list.
policy group	Enters webvpn group policy configuration mode to configure a group policy.
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

port-misuse

To permit or deny HTTP traffic through the firewall on the basis of specified applications in the HTTP message, use the **port-misuse** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

port-misuse {**p2p**| **tunneling**| **im**| **default**} **action** {**reset**| **allow**} **[alarm]**

no port-misuse {**p2p**| **tunneling**| **im**| **default**} **action** {**reset**| **allow**} **[alarm]**

Syntax Description

p2p	Peer-to-peer protocol applications subject to inspection: Kazaa and Gnutella.
tunneling	Tunneling applications subject to inspection: HTTPPort/HTTPHost, GNU Httptunnel, GotoMyPC, Firethru, Http-tunnel.com Client
im	Instant messaging protocol applications subject to inspection: Yahoo Messenger.
default	All applications are subject to inspection.
action	Applications detected within the HTTP messages that are outside of the specified application are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not enabled, HTTP messages are permitted through the firewall if any of the applications are detected within the message.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

ppp accounting through quit

ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

ppp accounting {**default**| *listname*}

no ppp accounting

Syntax Description

default	The name of the method list is created with the **aaa accounting** command.
listname	A specified method list.

Command Default

Accounting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	The *listname* argument was added.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the **ppp accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp accounting list1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no**form of this command.

ppp authentication *protocol1* [*protocol2...*] [**if-needed**| *list-name*| **default**| **callin**| **one-time**| **optional**]

no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the keywords described in the table below.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Name of the method list created with the **aaa authentication ppp** command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Command Default

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)	The **optional** keyword was added.
12.1(3)XS	The **optional** keyword was added.
12.2(2)XB5	Support for the **eap** authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
12.2(13)T	The **eap** authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When you enable Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp**command, you will disable PPP on this interface.

The table below lists the protocols used to negotiate PPP authentication.

Table 14: ppp authentication Protocols

chap	Enables CHAP on a serial interface.
eap	Enables EAP on a serial interface.
ms-chap	Enables MS-CHAP on a serial interface.
pap	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

Caution In Cisco IOS Release 15.0(1)S and later releases, enabling CHAP authentication only for incoming (received) calls is not supported in scenarios where the VPDN tunnel is established over a pseudowire, using the L2TP or L2TPv3 protocols. Enabling CHAP authentication only for incoming calls by using the **ppp authentication chap callin** command is not supported unless used in conjunction with the **ppp direction callout** command.

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
autoselect	Configures a line to start an ARAP, PPP, or SLIP session.
encapsulation	Sets the encapsulation method used by the interface.
ppp accm	Identifies the ACCM table.
ppp direction	Overrides the default direction of a PPP connection.
username	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

ppp authentication ms-chap-v2

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication on a network access server (NAS), use the **ppp authentication ms-chap-v2** command in interface configuration mode. To disable MSCHAP V2 authentication, use the **no** form of this command.

ppp authentication ms-chap-v2

no ppp authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Command Default

MSCHAP V2 authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable MSCHAP V2 authentication, first configure PPP on the NAS. For the NAS to properly interpret authentication failure attributes and vendor-specific attributes, the **ppp max-bad-auth**command must be configured to allow at least two authentication retries and the **radius-server vsa send**command and **authentication** keyword must be enabled. The NAS must be able to interpret authentication failure attributes and vendor-specific attributes to support the ability to change an expired password.

Examples

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
```

```
 ppp authentication ms-chap-v2
 username client password secret
```

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

Related Commands

Command	Description
debug aaa authentication	Displays information on AAA/TACACS+ authorization.
debug ppp	Displays information on traffic and exchanges in a network that is implementing PPP.
debug radius	Displays information associated with RADIUS.
ppp max-bad-auth	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
radius-server vsa send	Configures the network access server to recognize and use VSAs.

ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization**command in interface configuration mode. To disable authorization, use the no form of this command.

ppp authorization [**default**| *list-name*]

no ppp authorization

Syntax Description

default	(Optional) The name of the method list is created with the **aaa authorization** command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Command Default

Authorization is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4
```

```
encapsulation ppp
ppp authorization charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname**command ininterface configuration mode. To disable this function, use the **no** form of this command.

ppp chap hostname *hostname*

no ppp chap hostname *hostname*

Syntax Description

hostname	The name sent in the CHAP challenge.

Command Default

Disabled. The router name is sent in any CHAP challenges.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the Multilink PPP (MLP) bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Examples

The following example shows how to identify dialer interface 0 as the dialer rotary group leader and specify ppp as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username ISPCorp will be sent in all CHAP challenges and responses.

```
interface dialer 0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ISPCorp
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password**command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

ppp chap password *secret*

no ppp chap password *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Examples

The commands in the following example specify ISDN BRI number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0
 encapsulation ppp
 ppp chap password 7 1234567891
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse [callin]

no ppp chap refuse [callin]

Syntax Description

callin	(Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication.

```
interface bri 0
```

```
encapsulation ppp
ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

ppp chap wait *secret*

no ppp chap wait *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command (which is enabled by default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will respond immediately to an authentication challenge.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves.

```
interface bri 0
 encapsulation ppp
 no ppp chap wait
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.

ppp eap identity

To specify the Extensible Authentication Protocol (EAP) identity, use the **ppp eap identity** command in interface configuration mode. To remove the EAP identity from your configuration, use the **no** form of this command.

ppp eap identity *string*

no ppp eap identity *string*

Syntax Description

string	EAP identity.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.\
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap identity** command to configure the client to use a different identity when requested by the peer.

Examples

The following example shows how to enable EAP on dialer interface 1 and set the identity to “cat”:

```
interface dialer 1
 encapsulation ppp
 ppp eap identity cat
```

ppp eap local

To authenticate locally instead of using the RADIUS back-end server, use the **ppp eap local** command in interface configuration mode. To reenable proxy mode (which is the default), use the **no** form of this command.

ppp eap local

no ppp eap local

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication is performed via proxy mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelin

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

By default, Extensible Authentication Protocol (EAP) runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the **ppp eap local**command .

In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

Examples

The following example shows how to configure EAP to authenticate locally:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
 ppp eap local
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap password

To set the Enhanced Authentication Protocol (EAP) password for peer authentication, use the **ppp eap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp eap password [*number*] *string*

no ppp eap password [*number*] *string*

Syntax Description

number	(Optional) Encryption type, including values 0 through 7; 0 means no encryption.
string	Character string that specifies the EAP password.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For remote EAP authentication only, you can configure your router to create a common EAP password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor or from an older running version of the Cisco IOS software) to which a new (that is, unknown) router has been added, the common password will be used to respond to the new router. The **ppp eap password**command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

Examples

The following example shows how to set the EAP password “7 141B1309” on the client:

```
ppp eap identity user
ppp eap password 7 141B1309
```

ppp eap refuse

To refuse Enhanced Authentication Protocol (EAP) from peers requesting it, use the **ppp eap refuse** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp eap refuse [callin]

no ppp eap refuse [callin]

Syntax Description

callin	(Optional) Authentication is refused for incoming calls only.

Command Default

The server will not refuse EAP authentication challenges received from the peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap refuse** command to disable EAP authentication for all calls. If the **callin** keyword is used, the server will refuse to answer EAP authentication challenges received from the peer but will still require the peer to answer any EAP challenges the server sends.

Examples

The following example shows how to refuse EAP authentication on incoming calls from the peer:

```
ppp authentication eap
ppp eap local
ppp eap refuse callin
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap wait

To configure the server to delay the Enhanced Authentication Protocol (EAP) authentication until after the peer has authenticated itself to the server, use the **ppp eap wait** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ppp eap wait

no ppp eap wait

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap wait**command to specify that the server will not authenticate to a peer requesting EAP authentication until after the peer has authenticated itself to the server.

Examples

The following example shows how to configure the server to wait for the peer to authenticate itself first:

```
ppp authentication eap
ppp eap local
ppp eap wait
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp link

To generate the Point-to-Point Protocol (PPP) Link Control Protocol (LCP) down and keepalive-failure link traps or enable calls to the interface-reset vector, use the **ppp link**command in interface configuration mode. To disable the PPP LCP down and keepalive-failure link traps or calls to the interface-reset vector, use the **no** form of this command.

ppp link {**reset**| **trap**}

no ppp link {**reset**| **trap**}

Syntax Description

reset	Specifies calls to the interface reset vector.
trap	Specifies the PPP LCP down and keepalive-failure link traps.

Command Default

The defaults are as follows:

- The calls are sent to the interface-reset vector.
- The traps are sent when the LCP goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The **no ppp link trap** command disables the sending of the link traps when the LCP goes down.

In the event that the PPP calls the interface-reset vector while the LCP is configured or closed, Up/Down status messages will display on the console. If a leased-line configuration is up but the peer is not responding, PPP may call the interface-reset vector once per minute. This situation may result in the Up/Down status messages on the console. Use the **no ppp link reset**command to disable calls to the interface-reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Examples

This example shows how to enable calls to the interface-reset vector:

```
Router(config-if)#
ppp link reset
Router(config-if)#
```

This example shows how to disable calls to the interface-reset vector:

```
Router(config-if)#
no ppp link reset
Router(config-if)#
```

This example shows how to generate the PPP LCP down/keepalive-failure link traps:

```
Router(config-if)#
ppp link trap
Router(config-if)#
```

This example shows how to disable the sending of the link traps when the LCP goes down:

```
Router(config-if)#
no ppp link trap
Router(config-if)#
```

ppp pap refuse

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol (PAP), use the ppp pap refuse command in interface configuration mode. To disable the refusal, use the no form of this command.

ppp pap refuse

no ppp pap refuse

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to refuse remote PAP support; for example, to respond to the peer request to authenticate with PAP.

This is a per-interface command.

Examples

The following example shows how to enable the ppp pap command to refuse a peer request for remote authentication:

```
interface dialer 0 encapsulation ppp ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP and TACACS+.

Command	Description
encapsulation ppp	Sets PPP as the encapsulation method used by a serial or ISDN interface.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp pap sent-username	Reenables remote PAP support for an interface and uses the sent-username and password in the PAP authentication request packet to the peer.

ppp pap sent-username

To reenable remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** *password*

no ppp pap sent-username

Syntax Description

username	Username sent in the PAP authentication request.
password	Password sent in the PAP authentication request.
password	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

Command Default

Remote PAP support disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to reenable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

This is a per-interface command. You must configure this command for each interface.

Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. *ISPCorp*is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
```

```
ppp authentication chap pap callin
ppp chap hostname ISPCorp
ppp pap sent username ISPCorp password 7 fjhfeu
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.

preempt

To enable preemption on the redundancy group, use the **preempt**command in redundancy application group configuration mode. To disable the group's preemption, use the **no** form of this command.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the redundancy group.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to enable preemption on the redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) preempt
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
protocol	Defines a protocol instance in a redundancy group.

pre-shared-key

To define a preshared key to be used for Internet Key Exchange (IKE) authentication, use the **pre-shared-key**command in keyring configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**address** *address* [*mask*]| **hostname** *hostname*| **ipv6** {*ipv6-address*| *ipv6-prefix*}} **key** *key*

no pre-shared-key {**address** *address* [*mask*]| **hostname** *hostname*| **ipv6** {*ipv6-address*| *ipv6-prefix*}} **key** *key*

Syntax Description

address *address [mask]*	IP address of the remote peer or a subnet and mask. The *mask*argument is optional.
hostname *hostname*	Fully qualified domain name (FQDN) of the peer.
ipv6	Specifies that an IPv6 address of a remote peer will be used.
ipv6-address	IPv6 address of the remote peer. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	IPv6 prefix of the remote peer.
key *key*	Specifies the secret.

Command Default

None

Command Modes

Keyring configurati on (config-keyring)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(2)T	This command was modified so that output for the **pre-shared-key**command will show that the preshared key is either encrypted or unencrypted.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and the *ipv6-address* and *ipv6-prefix* arguments were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before configuring preshared keys, you must configure an Internet Security Association and Key Management Protocol (ISAKMP) profile.

Output for the **pre-shared-key** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key test123
```

An output example for a type 6 encrypted preshared key would be as follows:

pre-shared-key address 10.1.0.1 key 6 RHZE[JACMUI\bcbTdELISAAB

Examples

The following example shows how to configure a preshared key using an IP address and hostname:

```
Router(config)# crypto keyring vpnkeyring
Router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
Router(config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.

pre-shared-key (IKEv2 keyring)

To define a preshared key for an Internet Key Exchange Version 2 (IKEv2) peer, use the **pre-shared-key** command in IKEv2 keyring peer configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**local**| **remote**}[**0**| **6**| *line*| **hex** *hexadecimal-string*]

no pre-shared-key {**local**| **remote**}

Syntax Description

local	Specifies the signing key.
remote	Specifies the verifying key.
0	Specifies that the password is unencrypted.
6	Specifies that the password is encrypted.
line	Specifies an unencrypted user password.
hex *hexadecimal-string*	Specifies the preshared key is in hexadecimal format.

Command Default

The default is a symmetric key.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(3)T	This command was modified. The **hex** *hexadecimal-string* keyword-argument pair was added.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to specify the preshared key for the peer. Use the **local** or **remote** keywords to specify an asymmetric key.

Examples

The following examples show how to configure a preshared key in different scenarios.

Examples

The following is the keyring on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
```

The following is the keyring on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
```

Examples

The following is the keyring on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1 with asymmetric keys
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key local key-1
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-2
```

The following is the keyring on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2 with asymmetric keys
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key local key-2
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-1
```

Examples

The following is the keyring on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1 in abc domain
Router(config-ikev2-keyring-peer)# host host1.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key local key-1
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-2
```

The following is the keyring on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer host2
Router(config-ikev2-keyring-peer)# description host2 in example domain
Router(config-ikev2-keyring-peer)# host host2.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key local key-2
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-1
```

Examples

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-ikev2-keyring)# peer abc
Router(config-ikev2-keyring-peer)# description example domain
Router(config-ikev2-keyring-peer)# identity fqdn example.com
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-1
Router(config-ikev2-keyring-peer)# exit
Router(config-ikev2-keyring)# peer user1
```

```
Router(config-ikev2-keyring-peer)# description user1 in example domain
Router(config-ikev2-keyring-peer)# identity email user1@example.com
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-2
Router(config-ikev2-keyring-peer)# exit
Router(config-ikev2-keyring)# peer user1-remote
Router(config-ikev2-keyring)# description user1 abc remote users
Router(config-ikev2-keyring-peer)# identity key-id abc
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-3
```

Examples

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description ABCdomain
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key
```

Examples

The following is the configuration on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key hex 0x6A6B6C
```

The following is the configuration on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key jkl
```

Because the hexadecimal equivalent of each character in the string **jkl** is **0x6A6B6C**, the preshared key matches.

Related Commands

Command	Description
address (IKEv2 keyring)	Specifies the IPv4 address or the range of the peers in the IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (IKEv2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (IKEv2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
identity (IKEv2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.

prf

To specify one or more Pseudo-Random Function (PRF) algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **prf** command in IKEv2 proposal configuration mode. To remove the PRF algorithm, use the **no** form of this command.

prf *prf-algorithm...*

no prf

Syntax Description

prf-algorithm...	Specifies the type of PRF algorithm.

Command Default

The PRF algorithm is not specified.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.4(2)T	This command was introduced.
Cisco IOS XE Release 3.12S	This command was integrated into Cisco IOS XE Release 3.12S.

Usage Guidelines

Use this command to specify the PRF algorithm to be used in an IKEv2 proposal. The PRF algorithm can be one of the following:

PRF Type	Description
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the PRF algorithm.
sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the PRF algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the PRF algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the PRF algorithm.
sha512	Specifies SHA-2 family 512-bit (HMAC variant) as the PRF algorithm.

The PRF algorithm is required if the encryption type is Advanced Encryption Standard (AES) in Galois/Counter Mode (AES-GCM)**—aes-gmc-128** or **aes-gmc-256**, If the encryption algorithm is not AES-GCM, the PRF algorithm is the same as the specified integrity algorithm. However, you can specify a PRF algorithm, if required.

Examples

The following example configures an IKEv2 proposal with the 3DES encryption algorithm:

```
Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# encryption aes-cbc-256
Device(config-ikev2-proposal)# prf sha256 sha512
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (IKEv2 proposal)	Specifies one or more encryption algorithms for an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH group identifier in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

primary

To assign a specified trustpoint as the primary trustpoint of the router, use the **primary** command in ca-trustpoint configuration mode.

primary *name*

Syntax Description

name	Name of the primary trustpoint of the router.

Command Default

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the primary command to specify a given trustpoint as primary.

Before you can configure this command, you must enable the **crypto ca trustpoint**command , which defines the trustpoint and enters ca-trustpoint configuration mode.

Examples

The following example shows how to configure the trustpoint “ka” as the primary trustpoint:

```
cr
ypto ca trustpoint ka
 enrollment url http://xxx
 primary
 crl option
al
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

priority (firewall)

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode. To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]

no priority *value* [**failover-threshold** *value*]

Syntax Description

value	The priority value. The range is from 1 to 255.
failover-threshold *value*	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The priority of the redundancy group is used to determine a redundancy group's active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

private-hosts

To globally enable the Private Hosts feature, use the **private-hosts** command in global configuration mode. To disable the feature, use the **no** form of this command.

private-hosts

no private-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into the Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Issue this command to enable the Private Hosts feature on the router. Then, use the **private-hosts mode** command to enable Private Hosts on individual interfaces (ports).

Examples

The following example globally enables the Private Hosts feature on the router:

```
Router(config)# private-hosts
```

Related Commands

Command	Description
private-hosts mac list	Creates a MAC address list that identifies the content servers providing broadband services to isolated hosts.
private-hosts mode	Specifies the operating mode for a Private Hosts port.
private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

private-hosts layer3

To globally enable Layer 3 routing on private hosts, use the **private-hosts layer3** command in global configuration mode. To disable the feature, use the **no** form of this command.

private-hosts layer3

no private-hosts layer3

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.

Usage Guidelines

Use this command on the router to enable layer 3 routing on private hosts.

Examples

The following example shows the layer 3 configuration enabled on private hosts:

```
Router(config)# private-hosts layer3
Router(config)# end
Router# show private-hosts configuration
Private hosts disabled. BR INDEX 65536
Layer-3 switching on Private Hosts is enabled
Missing config: MAC list, VLAN list, MAC list association, Enable command, Atlea
st one Promiscuous/Mixed port
Privated hosts vlans lists:
None
```

Related Commands

Command	Description
private-hosts mac list	Creates a MAC address list that identifies the content servers providing broadband services to isolated hosts.
private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.

private-hosts mac-list

To identify the content servers that provide broadband services to isolated hosts, create a MAC address list by using the **private-hosts mac-list** command in global configuration mode. To delete an address from the MAC address list and remove that device from the list of content servers providing services for the Private Hosts feature, use the **no** form of this command.

private-hosts mac-list *mac-list-name mac-address* [**remark** *device-name*| *comment*]

no private-hosts mac-list *mac-list-name mac-address*

Syntax Description

mac-list-name	A name to assign to the address list (up to 80 characters).
mac-address	The MAC address of a Broadband Remote Access Server (BRAS), multicast server, or video server that provides broadband services for the Private Hosts feature. **Note** If the server is not directly connected to the networking device, specify the MAC address of the core network device that provides access to the server.
remark *device-name* | *comment*	(Optional) Specifies an optional device name or comment to assign to this MAC address list.

Command Default

The MAC address list is not populated with content servers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command creates a list of MAC addresses that identify the content servers being used to provide broadband services to isolated hosts in the Private Hosts configuration. The Private Hosts feature uses port-based Protocol-Independent MAC ACLs (PACLs) to provide Layer 2 isolation between hosts on trusted ports within a purely Layer 2 domain. The PACLs isolate the hosts by imposing Layer 2 forwarding constraints on the router ports.

Use this command to specify the MAC address of every content server that provides broadband services for the Private Hosts feature. A *content server* is any BRAS, multicast server, or video server that provides services to the isolated hosts in your network.

You can assign all of the content servers to a single MAC address list or you can create multiple MAC address lists, each identifying the content server for a particular type of broadband service or set of services. When you configure the promiscuous ports for Private Hosts, you specify a MAC address list and VLAN list to identify the server and receiving hosts for broadband services.

If you plan to deliver different types of broadband services to different sets of hosts, create multiple MAC address lists to identify the servers for each type of service. You can also create multiple VLAN lists to identify different sets of isolated hosts. When you configure promiscuous ports, you can specify different combinations of MAC address lists and VLAN lists to identify the servers and receiving hosts for each type of service.

Note The MAC address list is deleted when the last address in the list is deleted.

Examples

This example creates a MAC address list named BRAS1 that identifies the MAC address of the upstream BRAS. The optional remark names the MAC address list BRAS1.

```
Router(config)# private-hosts mac-list BRAS1 0000.1111.1111 remark BRAS1
```

Related Commands

Command	Description
show private-hosts mac-list	Displays a list of the MAC addresses that identify the content servers that are providing broadband defined for Private Hosts.

private-hosts mode

To enable Private Hosts on an interface (port) and specify the mode in which the port is to operate, use the **private-hosts mode** command in interface configuration mode. To disable Private Hosts on the port, use the **no** form of this command.

private-hosts mode {**promiscuous| isolated| mixed**}

no private-hosts

Syntax Description

promiscuous	Configures the port for promiscuous mode. Use this mode for ports that face upstream. These are the ports that connect the router to the servers providing broadband services (Broadband Remote Access Server [BRAS], multicast, or video), or to the core network devices providing access to the servers.
isolated	Configures the port for isolated mode. Use this mode for ports that face the DSL access multiplexer (DSLAM) to which the isolated hosts are connected.
mixed	Configures the port for mixed mode. Use this mode for ports that connect to other networking devices, typically in a ring topology. The behavior of this port can change depending on the Spanning Tree Protocol (STP) topology.

Command Modes

This command is disabled by default. The default for the **mode** keyword is promiscuous.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you can use this command, you must globally enable the Private Hosts feature on the router by issuing the **private-hosts** command.

Use this command to enable the Private Hosts feature on individual ports and to define the mode of operation for the port. A port's mode determines which type of Protocol-Independent MAC ACLs (PACL) will be

assigned to the port in order to restrict the type of traffic that is allowed to pass through the port. Each type of PACL restricts the traffic flow for a different type of traffic (for example, from content servers to isolated hosts, from isolated hosts to servers, and traffic between isolated hosts). Use the **show private-hosts interface configuration** command to display the mode assigned to Private Hosts ports.

Examples

The following command example enables Private Hosts on an interface (port) and configures the port for isolated mode:

```
Router(config-if)# private-hosts mode isolated
```

Related Commands

Command	Description
private-hosts	Enables or configures the private hosts feature.
show fm private-hosts	Displays the FM-related private hosts information.
show private-hosts	Displays the private hosts information.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts promiscuous

To identify the content servers and receiving hosts for broadband services, use the **private-hosts promiscuous** command in global configuration mode. To remove a promiscuous ports setting, use the **no** form of this command.

private-hosts promiscuous *mac-list-name* [**vlan** *vlan-ids*]

no private-hosts promiscuous *mac-list-name*

Syntax Description

mac-list-name	The name of MAC address list that identifies the content servers (Broadband Remote Access Server [BRAS], multicast, or video) providing broadband services for the Private Hosts feature.
vlan *vlan-ids*	(Optional) The VLAN or set of VLANs whose hosts will be allowed to receive services from the content servers identified by the MAC address list. Use commas to separate individual VLANs and hyphens to specify a range of VLANs (for example, 1,3,5,20-25). **Note** If no VLAN list is specified, the global VLAN list is used.

Command Default

Promiscuous ports are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The MAC address list and VLAN list define the content servers and receiving hosts for broadband services. If no VLAN list is specified, the system uses the global VLAN list created with the **private-hosts vlan-list** command.

You can issue this command multiple times to specify multiple combinations of MAC and VLAN lists, each defining the server and receiving hosts for a particular type of service. For example, the BRAS at xxxx.xxxx.xxxx could be used to deliver a basic set of services over VLANs 20, 25, and 30, and the BRAS at yyyy.yyyy.yyyy could be used to deliver a premium set of services over VLANs 5, 10, and 15.

Examples

The following example configures the broadband services provided by the content servers defined in the BRASlist address list to be delivered to the isolated hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts promiscuous BRASlist vlan 10,12,15,200-300
```

Related Commands

Command	Description
private-hosts vlan-list	Creatse a VLAN list to be used to identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services).
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts vlan-list

To create a VLAN list to be used to identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services) use the **private-hosts vlan-list** command in global configuration mode. To remove a VLAN from the list of VLANs requiring host isolation, use the **no** form of this command.

private-hosts vlan-list *vlan-ids*

no private-hosts vlan-list *vlan-ids*

Syntax Description

vlan-ids	A list of the VLANs whose hosts need to be isolated from each other. Use commas to separate individual VLANs and hyphens to specify a range of VLANs (for example, 1,3,5,20-25).

Command Default

A VLAN is not included in the list of VLANs requiring host isolation.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command creates a list of VLANs whose hosts need to be isolated through the Private Hosts feature. The VLAN list should include all of the VLANs that are being used to deliver broadband services to multiple end users (isolated hosts).

If you plan to deliver different types of broadband services to different sets of hosts, you can create multiple VLAN lists and multiple MAC address lists. When you configure promiscuous ports, you can specify different combinations of MAC and VLAN lists to identify the content servers and receiving hosts for each type of service.

If you do not specify a VLAN list when you configure promiscuous ports, the system uses the global VLAN list created by this command.

Note The Private Hosts feature isolates the hosts in all of the VLANs included in VLAN lists; therefore, VLAN lists should include only those VLANs that are being used to deliver broadband services.

Examples

This example shows how to configure the Private Hosts feature to isolate the hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts vlan-list 10,12,15,200-300
```

Related Commands

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.

privilege

To configure a new privilege level for users and associate commands with that privilege level, use the **privilege**command in global configuration mode. To reset the privilege level of the specified command or commands to the default and remove the privilege level configuration from the running configurationfile, use the **no**form of this command.

Note As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

privilege *mode* **[all]** {**level** *level*| **reset**} *command-string*

no privilege *mode* **[all]** {**level** *level*| **reset**} *command-string*

Syntax Description

mode	Configuration mode for the specified command. See the table in the "Usage Guidelines" section for a list of options for this argument.
all	(Optional) Changes the privilege level for all the suboptions to the same level.
level *level*	Specifies the privilege level you are configuring for the specified command or commands. The level argument must be a number from 0 to 15.
reset	Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running configuration file. **Note** For Cisco IOS software releases earlier than Release 12.3(6) and Release 12.3(6)T, you use the **no** form of this command to reset the privilege level to the default. The default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the **reset** keyword.
command-string	Command associated with the specified privilege level. If the **all** keyword is used, specifies the command and subcommands associated with the privilege level.

Command Default

User EXEC mode commands are privilege level 1.

Privileged EXEC mode and configuration mode commands are privilege level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(22)S, 12.2(13)T	The **all** keyword was added.
12.3(6), 12.3(6)T	The **no** form of the command performs the same function as the **reset** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The password for a privilege level defined using the **privilege**global configuration command is configured using the **enable secret**command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users**and **exit** commands.

Note There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip**commands are automatically set to privilege level 15--unless you set them individually to different levels. This is necessary because you can’t execute, for example, the **show ip** command unless you have access to **show** commands.

To change the privilege level of a group of commands, use the **all** keyword. When you set a group of commands to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if you set the **show ip** keywords to level 5, show and ip will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

The table below shows some of the keyword options for the mode argument in the **privilege**command. The available mode keywords will vary depending on your hardware and software version. To see a list of available mode options on your system, use the **privilege ?**command.

Table 15: mode Argument Options

Command	Description
accept-dialin	VPDN group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address Family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signalling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request Configuration
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map config mode
crypto-transform	Crypto transform config modeCrypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	Exec mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode

Command	Description
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map class configuration mode
map-list	Map list configuration mode
mpoa-client	MPOA Client
mpoa-server	MPOA Server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode
route-map	Route map configuration mode
router	Router configuration mode
rsvp_policy_local	
rtr	RTR Entry Configuration
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode

Command	Description
vc-class	VC class configuration mode
voiceclass	Voice Class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial Peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands:

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

The following example shows how to set the **show**and **ip**keywords to level 5. The suboptions coming under **ip** will also be allowed to users with privilege level 5 access:

```
Router(config)# privilege exec all level 5 show ip
```

The following two examples demonstate the difference in behavior between the **no** form of the command and the use of the **reset** keyword when using Cisco IOS software releases earlier than Releases 12.3(6) and Release 12.3(6)T.

Note As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

```
! show currently configured privilege commands
Router# show running-config | include priv

privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no privilege exec level 3 configure terminal
Router(config)# end
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 15 configure terminal
privilege exec level 15 configure
```

Note that in the **show running-config**output above, the privilege command for “configure terminal” still appears, but now has the default privilege level assigned.

To remove a previously configured privilege command entirely from the configuration, use the **reset** keyword, as shown in the following example:

```
! show currently configured privilege commands
Router# show running-config | include priv
```

```
privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# privilege exec reset configure terminal
Router(config)#
Router# show running-config | include priv

privilege configure all level 3 interface
Router#
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege level	Sets the default privilege level for a line.

privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

privilege level *level*

no privilege level

Syntax Description

level	Privilege level associated with the specified line.

Command Default

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict line usage.

Note Before Cisco IOS Release 12.2SXI, it was mandatory that a privilege level of 15 needed to be configured in the Access Control System (ACS) for Webauth (web authentication) to succeed. After this release, privilege configurations in the ACS are no longer mandatory.

Note Some CLI commands are not supported with the **privilege level** command. For example, commands such as **router bgp**, and **default interface**, etc cannot be associated with a privilege level. Though the global configuration CLI may accept the privilege-level assignment for these unsupported commands, they do not become part of the router's running-configuration.

Examples

The following example configures the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:

```
line aux 0
 privilege level 5
```

The following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The following example sets the **show ip route** command to level 7 and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

profile (GDOI local server)

To define the IP security (IPsec) security association (SA) policy for a Group Domain of Interpretation (GDOI) group, use the **profile** command in GDOI local server configuration mode. To disable the IPsec SA policy that was defined, use the **no** form of this command.

profile *ipsec-profile-name*

no profile *ipsec-profile-name*

Syntax Description

ipsec-profile-name	Name of the IPsec profile.

Command Default

An IPsec SA policy is not defined for the GDOI group.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example shows that the IPsec SA policy has been defined as “group1234”:

```
profile group1234
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

profile (profile map configuration)

To define or modify an individual authentication and authorization cache profile, use the **profile** command in profile map configuration mode. To disable a cache profile, use the **no** form of this command.

profile *name* **[no-auth]**

no profile *name*

Syntax Description

name	Text string that is an exact match to an existing username.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No profiles are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **profile** command to define or modify an authentication and authorization cache profile. The *name* argument in this command must be an exact match to a username being queried by an authentication or authorization service request.

Using the **profile** command with the *name* argument, as opposed to using the **regexp** or **all** command, is the recommended way to cache information.

Examples

The following example defines a cache profile that includes no user authentication and is a part of the localusers cache profile group:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# profile user101 no auth
```

Related Commands

Command	Description
aaa cache profile	Creates a named authentication and authorization cache profile group.
all	Specifies that all authentication and authorization requests be cached.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

propagate sgt

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

Command History

Release	Modification
4.1(2)	This command was introduced on the Cisco Nexus 7000 series switches.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S.

Usage Guidelines

SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

Examples

The following example shows how to disable SGT propagation on Gigabit Ethernet interface 0:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# cts manual
Router(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
Router#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Disabled
```

```
Cache Info:
    Cache applied to link : NONE
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
show cts interface	Displays information about CTS interfaces.

propagate sgt (config-if-cts-dot1x)

To enable Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface, use the **propagate sgt** command in CTS dot1x interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

no propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS dot1x interface configuration (config-if-cts-dot1x)

Command History

Release	Modification
12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

SGT propagation (SGT tag encapsulation) is enabled by default in both CTS dot1x and CTS manual interface configuration modes. A TrustSec-capable port can support Layer-2 MACsec and SGT encapsulation, and negotiates the most secure mode with the peer for the transmittal of the SGT tag and data. MACsec is an 802.1AE standard-based link-to-link protocol used by switches and servers. A peer can support MACsec, but not SGT encapsulation. In such a case, it is recommended that this Layer 2 SGT propagation be disabled with the **no propagate sgt** CTS Dot1x interface configuration command.

To re-enable the SGT propagation enter the **propagate sgt** command. Use the **show cts interface** command to verify the state of SGT propagation. Only the disabled state is saved in the nonvolatile generation (NVGEN) process.

Examples

The following example enables SGT propagation on a TrustSec-capable interface:

```
Device(config)# interface gigabit 6/1
Device(config-if)# cts dot1x
Device(config-if-cts-dot1x)# propagate sgt
Device# show cts interface gigabit 6/1

Global Dot1x feature is Enabled

Interface GigabitEthernet6/1:

    CTS is enabled, mode:    DOT1X

    IFC state:               INIT
```

```
SAP Status:              UNKNOWN
Configured pairwise ciphers:
 gcm-encrypt
 null
        Replay protection:      enabled
        Replay protection mode: STRICT
        Selected cipher:
    Propagate SGT:           Enabled
```

Related Commands

Command	Description
cts dot1x	Enables Network Device Admission Control (NDAC) and configure NDAC authentication parameters.
sap mode-list (config-if-cts-dot1x)	Configures CTS Security Association Protocol (SAP) authentication.
show cts interface	Displays CTS interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.
timer reauthentication (config-if-cts-dot1x)	Configures the reauthentication timer for a CTS device.

proposal

To specify the proposals in an Internet Key Exchange Version 2 (IKEv2) policy, use the **proposal** command in IKEv2 policy configuration mode. To delete the proposal from the policy, use the **no** form of this command.

proposal *name*

no proposal *name*

Syntax Description

name	Proposal name.

Command Default

The default proposal is used with the default policy.

Command Modes

IKEv2 policy configuration (config-ikev2-policy)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this option to specify the proposals to use with the policy. One proposal must be specified at least and additional proposals can be specified with one proposal for each statement. The proposals are prioritized in the order of listing.

Note The specified proposals must be defined. Use the **crypto ikev2 proposal** command to define a proposal.

Examples

The following example shows how to specify a proposal in an IKEv2 policy:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
```

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.

Command	Description
crypto ikev2 proposal	Defines an IKE proposal.
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
show crypto ikev2 policy	Displays the default or user-defined IKEv2 policy.

protection (zone)

To configure TCP synchronization (SYN) cookie protection against SYN-flood attacks, use the **protection** command in security zone configuration mode. To disable the SYN cookie protection, use the **no** form of this command.

protection *parameter-map-name*

no protection *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

SYN cookie protection is not configured.

Command Modes

Security zone configuration (config-sec-zone)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

You must configure the **zone security** command before you can configure the **protection** command.

You can use the **protection** command to bind an inspect zone-type parameter map to a zone.

TCP SYN-flooding attacks are a type of denial-of-service (DoS) attack. Usually, TCP SYN packets are sent to a targeted end host or a range of subnet addresses behind the firewall.

Examples

The following example shows how to configure the TCP SYN cookie protection:

```
Router(config)# zone security zone1
Router(config-sec-zone)# protection zone-pmap
Router(config-sec-zone)# end
```

Related Commands

Command	Description
zone security	Creates a security zone and enters security zone configuration mode.

protocol

To define a protocol instance in a redundancy group, use the **protocol**command in redundancy application configuration mode. To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*

no protocol *id*

Syntax Description

id	Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.

Command	Description
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

protocol (config-filter-list)

To specify a protocol instance in a sensor protocol filter list, use the **protocol** command in filter list configuration mode. To remove the protocol instance form the sensor protocol filter list, use the **no** form of this command.

protocol *protocol-name*

no protocol *protocol-name*

Syntax Description

protocol-name	Specifies the protocol name. Valid values are: • **cdp** • **dhcp** • **h323** • **http** • **lldp** • **mdns** • **sip**

Command Default

A protocol instance is not specified in the sensor protocol filter list.

Command Modes

Filter list configuration (config-filter-list)

Command History

Release	Modification
15.2(2)E	This command was introduced prior to Cisco IOS Release 15.2(2)E.

Examples

The following example shows how to configure a protocol instance in a sensor protocol filter list:

```
Device# configure terminal
Device(config)# access-session accounting attributes filter-list list mylist
Device(config-filter-list)# protocol http
Device(config-filter-list)# end
```

Related Commands

Command	Description
access-session accounting	Adds access-session protocol data to accounting records and generates additional accounting events when new sensor data is detected.

proxy

To configure proxy parameters for an Easy VPN remote device, use the **proxy** command in ISAKMP browser proxy configuration mode. To disable the parameters, use the **no** form of this command.

proxy *proxy-parameter*

no *proxy-parameter*

Syntax Description

proxy-parameter	Proxy parameter. See the table below for a list of acceptable proxy parameters.

Command Default

Proxy parameters are not set.

Command Modes

ISAKMP browser proxy configuration (config-ikmp-browser-proxy)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a subcommand of the **crypto isakmp client configuration browser-proxy** command.

The table below lists acceptable proxy parameters.

Table 16: Proxy Parameters

Proxy Parameter	Result
auto-detect	Automatically detects proxy settings.
by-pass-local	Bypasses proxy server for local addresses.
exception-list	Semicolon- (;) delimited list of IP addresses.
none	No proxy settings.

Proxy Parameter	Result
server	Proxy server IP and port number (ip:port number).

Examples

The following example shows various browser-proxy parameter settings for a browser proxy named “bproxy.”:

```
crypto isakmp client configuration browser-proxy bproxy
 proxy auto-detect
crypto isakmp client configuration browser-proxy bproxy
 proxy none
crypto isakmp client configuration browser-proxy bproxy
 proxy server 10.1.1.1:2000
 proxy exception-list 10.2.2.*,www.*org
 proxy by-pass-local
```

Related Commands

Command	Description
crypto isakmp client configuration browser-proxy	Configures browser-proxy parameters for an Easy VPN remote device.

publickey

To configure the location of the 512-byte public key that is used for encrypting the session key used for Cloud Web Security header encryption, use the **publickey** command in parameter-map type inspect configuration mode. To remove the location of the public key, use the **no** form of this command.

publickey *filesystem*

no publickey *filesystem*

Syntax Description

filesystem	The location of the local file system.

Command Default

The location of the public key for encryption is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The Cisco IOS Release 15.2(1)T supports only local file systems such as slot, disk, flash, nvram, and so on.

Examples

The following example shows how to configure the flash file system as the location of the public key:

```
Device(config)# parameter-map type cws global
Device(config-profile)# publickey flash:
```

Related Commands

Command	Description
parameter-map type inspect cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

qos-group (PVS Bundle Member)

To associate a quality of service (QoS) group or groups with a permanent virtual circuit (PVC) bundle-member, use the **qos-group**command in PVC bundle member configuration mode. To remove a QoS-group from a PVC bundle member, use the **no** form of this command.

qos-group *group number*

no qos-group *group number*

Syntax Description

group number <0-99>	Associates a QoS-group with a PVC bundle member. You can associate one QoS group, a range of QoS groups, or any combination of QoS groups and ranges of QoS groups, separated by commas, with a PVC bundle member. When a range of QoS groups is associated with a PVC bundle, only the starting and ending QoS group number need to be listed, separated by a hyphen. For example, 1-5. When multiple-non contiguous QoS groups or non-contiguous ranges of QoS groups are associated with a PVC bundle, separate the groups. For example, 1, 3, 8-10, 12-14. When a QoS group is associated with a bundle member, use a number from 0 to 99. When a QoS group is not associated with a PVC bundle, use numbers greater 100 and greater.
other	All non-configured QoS groups.

Command Default

By default, QoS groups are not associated with PVC bundle members.

Command Modes

PVC bundle-member configuration mode

Command History

Release	Modification
12.4(4)T	This command was introduced to associate a QoS-group with a permanent virtual circuit (PVC) bundle member, using the **qos-group** command in ATM VC bundle-member configuration mode.
12.2(31)SB2	This command was integrated into the Cisco IOS Release 12.2(31)SB2.

Release	Modification
12.4(9)XJ	This command modification was integrated into the Cisco IOS Special Release 12.4(9)XJ.
12.4(15)T	This command modification was integrated into the Cisco IOS Release 12.4(6th)T and associates a QoS-group with a permanent virtual circuit (PVC) bundle member in PVC bundle member configuration mode.

Examples

The following example shows the configuration of which QoS groups will use RBE:

```
Router(config-if-atm-member)# qos group 5
```

query certificate

To configure query certificates on a per-trustpoint basis, use the **query certificate** command in ca-trustpoint configuration mode. To disable creation of query certificates per trustpoint, use the **no** form of this command.

query certificate

no query certificate

Syntax Description

This command has no arguments or keywords.

Command Default

Query certificates are stored in NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was incorporated into Relese 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to prevent certificates from being stored locally; instead, they are retrieved from a specified certification authority (CA) trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

Before you can configure this command, you must enable the **crypto ca trustpoint**command , which puts you in ca-trustpoint configuration mode.

Using the query certificate Command with a Specific Trustpoint

When the **query certificate** command is used, certificates associated with the specified truspoint will not be written into NVRAM, and the certificate query will be attempted during the next reload of the router.

Applying the Query Mode Globally

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certicate query** command is used, any previously query certificate configuration will be removed from all trustpoints, and any query in progress will be halted and the feature disabled.

Examples

The following example shows how to configure a trustpoint and initiate query mode for certificate authority:

```
crypto ca trustpoint trustpoint1
```

```
enrollment url http://trustpoint1
crl query ldap://trustpoint1
query certificate
exit
```

Related Commands

Command	Description
crypto ca certificate query	Specifies that certificates should not be stored locally but retrieved from a CA trustpoint.
crypto ca trustpoint	Declares the CA that your router should use.

query url

Note Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **crl query** command.

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **query url**command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete (LDAP) URL, use **no** form of this command.

query url ldap://*hostname***:**[*port*]

noquery url ldap://*hostname*[**:**[*port*]]

Syntax Description

ldap **://** hostname	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
: port	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

Command Default

No enabled. If **query url ldap ://** *hostname* **:**[*port*] is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap:myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	This command was replaced by the **crl query** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example1: http://10.10.10.10:81/myca.crl)
- LDAP URL (Example 2: ldap://10.10.10.10:3899/CN=myca, O=cisco or Example 3: ldap:///CN=myca, O=cisco)
- LDAP/X.500 DN (Example 4: CN=myca, O=cisco)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The **ldap://** *hostname* **:**[*port*} keywords and arguments are used to provide this information.

Note The **crypto ca trustpoint**commandreplaces the **crypto ca identity**and **crypto ca trusted-root**commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, theconfiguration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint mytp
 enrollment url http://bar.cisco.com
 query url ldap://bar.cisco.com:3899
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

quit

To exit from the key-string mode while defining the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **quit** command in public key configuration mode.

quit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to exit text mode while defining the RSA public key.

Examples

The following example shows that the RSA public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.

radius attribute nas-port-type through rd

radius attribute nas-port-type

To configure subinterfaces such as Ethernet, virtual LANs (VLAN), stacked VLAN (Q-in-Q), virtual circuit (VC), and VC ranges, use the **radius attribute nas-port-type** command in subinterface configuration mode. To disable the subinterface configuration, use the **no** form of this command.

radius attribute nas-port-type *port number*

no radius attribute nas-port-type *port number*

Syntax Description

value	Number assigned for a port type. • The *port number*must be assigned a number 1-40 to set a customized extended NAS-Port Type and configure a specific service port type. Choosing a number outside of this range will force the default NAS port format e string to be used to configure the value for attribute 5 that is sent for that session. • You can set a specific service port type with the **radius-server attribute nas-port format** command. **Note** This setting will override a global NAS-Port-Type session format.

Command Default

NAS-Port-Type is not configured.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.3(7)XI	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

You can override the attribute 61 configured globally at a subinterface level.

To set a different extended attribute 61 value for a subinterface, such as for Ethernet, VLAN, Q-in-Q, VC, or VC ranges, select a value for that port type. An extended attribute 61 setting at a subinterface level will override the global extended attribute 61 value.

Examples

The following example shows how to override the global value set for an extended attribute 61 by setting a separate value of type 30 (PPP over ATM [PPPoA]) on a specific ATM subinterface:

```
Router# configure terminal
Router(config)#
Router(config)# interface atm 5/0/0.1
Router(config-subif)# pvc 1/33
Router(config-if-atm-vc)#
Router(config-if-atm-vc)# radius attribute nas-port-type 30
```

Related Commands

Command	Description
radius-server attribute 61 extended	Enables extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61).
radius-server attribute nas-port format	Sets the NAS-Port format used for RADIUS accounting features and restores the default NAS-Port format, or sets the global attribute 61 session format e string or configures a specific service port type for attribute 61 support.

radius ip-input-bypass

To enable an incoming RADIUS packet to bypass the IP path, use the **radius ip-input-bypass** command in global configuration mode. To disable the RADIUS packet bypass configuration, use the **no** form of this command.

radius ip-input-bypass

no radius ip-input-bypass

Syntax Description

This command has no arguments or keywords.

Command Default

The incoming RADIUS packet is enabled to bypass the IP path.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **radius ip-input-bypass** command to let the incoming RADIUS packets bypass the IP path in the device. The bypass configuration reduces the overall latency and helps packets reach the RADIUS module in the device faster.

Examples

The following example shows how to configure a RADIUS packet that bypasses the IP path:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius ip-input-bypass
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

radius server

To specify the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, use the **radius server** command in global configuration mode. To delete the specified RADIUS server configuration name, use the **no**form of this command.

radius server *name*

no radius server *name*

Syntax Description

name	Name of the RADIUS server configuration for PAC provisioning.

Command Default

No RADIUS server configuration name for PAC provisioning is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **radius server** command enters RADIUS server configuration mode where PAC provisioning parameters can be configured for the named RADIUS server. The **aaa new-model** command must be configured before accessing this command.

To check the available options in this mode, type **?** after entering into RADIUS server configuration mode (config-radius-server).

The following options are available:

- **address—**The RADIUS server address
- **automate-tester—**Configure automated testing for the server
- **backoff—**Configure the router for backoff retransmission of accounting requests per RADIUS server or server group
- **exit—**Exit from RADIUS server configuration mode
- **key—**Per-server encryption key
- **no—**Negate a command or set its defaults
- **non-standard—**Identify attributes to be parsed that violate the RADIUS standard
- **pac—**Protected Access Credential key

- **retransmit—**Number of retries of a RADIUS request to an active server
- **timeout—**Time to wait (in seconds) for the RADIUS server to reply

Examples

The following example shows the configuration of RADIUS server accounting and authentication parameters for PAC provisioning and the specification of the PAC key:

```
Router(config)# aaa new-model
Router(config)# radius server
Router(config-radius-server)# address ipv4 10.0.0.1 acct-port 1813 auth-port 1812
Router(config-radius-server)# pac key 7 mypackey
```

The following example shows how to configure a RADIUS server on a Cisco Aggregation Services Router (ASR):

```
aaa group server radius DU-radius
 server name scabbers
 server name pigwidgeon
 accounting system host-config
 ip radius source-interface Loopback102
!
aaa authentication ppp default group DU-radius
 interface Loopback102
 description BORDER-Loopback
 ip address 209.165.200.225 255.255.255.0
 no ip redirects
!
radius server pigwidgeon
 address ipv4 192.0.2.1 auth-port 1645 acct-port 1646
 retransmit 2
 key DUqwestDSL
!
radius server scabbers
 address ipv4 192.0.2.1 auth-port 1645 acct-port 1646
 retransmit 2
 key DUqwestDSL
```

Related Commands

Command	Description
aaa new-model	Enables new RADIUS and AAA access control commands and functions and disables old commands.
address ipv4	Configures the RADIUS server accounting and authentication parameters for PAC provisioning.
pac key	Specifies the PAC encryption key (overrides the default).

radius-server accounting system host-config

To enable the router to send a system accounting record for the addition and deletion of a RADIUS server, use the **radius-server accounting system host-config**command in global configuration mode.

To to disable system accounting records, use the **no** form of this command:

radius-server accounting system host-config

no radius-server accounting system host-config

Command Default

The *command-level defaul* t is not enabled.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
12.4	This command was introduced in Cisco IOS Release 12.4.

Usage Guidelines

The **radius-server accounting system host-config** command is used when configuring RADIUS system accounting on the global RADIUS server.

Examples

The following example shows how RADIUS system accounting is configured with the **radius-server accounting system host-config command to enable**system accounting records on a RADIUS server and private server hosts when they are added or deleted:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# radius-server accounting system host-config
Router(config)# aaa group server radius radgroup1
Router(config-sg-radius)# server-private 172.16.1.11 key cisco
Router(config-sg-radius)# accounting system host-config
```

Related Commands

Command	Description
aaa new-model	Enables AAA network security services.
aaa group server radius	Adds the RADIUS server
server-private	Enters the hostname or IP address of the RADIUS server and hidden server key.

Command	Description
accounting system host-config	Enables the generation of system accounting records for private server hosts when they are added or deleted.

radius-server attribute 4

To configure an IP address for the RADIUS attribute 4 address, use the **radius-server attribute 4** command in global configuration mode. To delete an IP address as the RADIUS attribute 4 address, use the **no** form of this command.

radius-server attribute 4 *ip-address*

no radius-server attribute 4 *ip-address*

Syntax Description

ip-address	IP address to be configured as RADIUS attribute 4 inside RADIUS packets.

Command Default

If this command is not configured, the RADIUS NAS-IP-Address attribute will be the IP address on the interface that connects the network access server (NAS) to the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(3)B	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Normally, when the **ip radius-source interface** command is configured, the IP address on the interface that is specified in the command is used as the IP address in the IP headers of the RADIUS packets and as the RADIUS attribute 4 address inside the RADIUS packets.

However, when the **radius-server attribute 4** command is configured, the IP address in the command is used as the RADIUS attribute 4 address inside the RADIUS packets. There is no impact on the IP address in the IP headers of the RADIUS packets.

If both commands are configured, the IP address that is specified in the **radius-server attribute 4** command is used as the RADIUS attribute 4 address inside the RADIUS packets. The IP address on the interface that is specified in the **ip radius-source interface** command is used as the IP address in the IP headers of the RADIUS packets.

Some authentication, authorization, and accounting (AAA) clients (such as PPP, virtual private dial-up network [VPDN] or Layer 2 Tunneling Protocol [L2TP], Voice over IP [VoIP], or Service Selection Gateway [SSG])

may try to set the RADIUS attribute 4 address using client-specific values. For example, on an L2TP network server (LNS), the IP address of the L2TP access concentrator (LAC) could be specified as the RADIUS attribute 4 address using a VPDN or L2TP command. When the **radius-server attribute 4** command is configured, the IP address specified in the command takes precedence over all IP addresses from AAA clients.

During RADIUS request retransmission and during RADIUS server failover, the specified IP address is always chosen as the value of the RADIUS attribute 4 address.

Examples

The following example shows that the IP address 10.0.0.21 has been configured as the RADIUS NAS-IP-Address attribute:

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

The following **debug radius** command output shows that 10.0.0.21 has been successfully configured.

```
Router# debug radius
RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
UDP: sent src=11.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS(0000001C): Received from id 21645/17
```

Related Commands

Command	Description
ip radius-source interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

radius-server attribute 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6**command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 {**mandatory**| **on-for-login-auth**| **support-multiple**| **voice** *value*}

no radius-server attribute 6 {**mandatory**| **on-for-login-auth**| **support-multiple**| **voice** *value*}

Syntax Description

mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.
on-for-login-auth	Sends the Service-Type attribute in the authentication packets. **Note** The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include "Service-Type=Outbound" as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.
voice *value*	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.

Command Default

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The **mandatory** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

The **support-multiple** keyword allows for multiple instances of the Service-Type attribute to be present in an Access-Accept packet. The default behavior is to disallow multiple instances, which results in an Access-Accept packet containing multiple instances being treated as though an Access-Reject was received.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router(config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router(config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router(config)# radius-server attribute 6 support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router(config)# radius-server attribute 6 voice 1
```

radius-server attribute 8 include-in-access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include-in-access-req** command in global configuration mode. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

radius-server attribute 8 include-in-access-req

no radius-server attribute 8 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Command Default

The user IP address is not sent to the RADIUS server during authentication.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 8 include-in-access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the username, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.
- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and stop packets will also include the same IP address as in attribute 8.

Note Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

However, the RADIUS attribute 8 (Framed-IP-Address) is not included in the accounting start packets in the following two scenarios:

- The user is a dual-stack (IPv4 or IPv6) subscriber.
- The IP address is from a local pool and not from the RADIUS server.

In both scenarios, use the **aaa accounting delay-start extended-time** *delay-value* command to delay the Internet Protocol Control Protocol Version 6 (IPCPv6) address negotiation using the configured delay value. During the delay, the IPCPv4 address is sent to the RADIUS server and the Framed-IP-Address attribute is added to the accounting start packet.

Examples

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa accounting delay-start	Specifies delay generation of accounting start records until the user IP address is established.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

radius-server attribute 11 default direction

To specify the default direction of filters from RADIUS, use the **radius-server attribute 11 default direction**command in global configuration mode. To remove this functionality from your configuration, use the **no** form of this command.

radius-server attribute 11 default direction [**inbound**| **outbound**]

no radius-server attribute 11 default direction [**inbound**| **outbound**]

Syntax Description

inbound	(Optional) Filtering is applied to inbound packets only.
outbound	(Optional) Filtering is applied to outbound packets only.

Command Default

This command is disabled by deault.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 11 default direction**command to change the default direction of filters from RADIUS (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user). Enabling this command allows you to change the filter direction to inbound--which stops traffic from entering a router and prevents resource consumption--rather than keeping the outbound default direction, where filtering occurs only as the traffic is about to leave the network.

Examples

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

```
radius-server attribute 11 default direction inbound
```

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "password1"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Filter-Id = "myfilter.out"
```

radius-server attribute 25

To include the class attribute in access-request, use the **radius-server attribute 25**command in global configuration mode. To disable class RADIUS configuration, use the **no** form of this command.

radius-server attribute 25 access-request include

no radius-server attribute 25 access-request include

Syntax Description

access-request	Specifies the default authorization action.
include	Specifies the framed-protocol attribute type.

Command Default

The class atrribute in access-request is not included.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Attribute 25 refers to class attribute.

Examples

The following example shows how to include the class attribute in access-request:

```
Router# configure terminal
Router(config)# radius-server attribute 25 access-request include
```

Related Commands

Command	Description
radius-server attribute 11 direction default	Specifies the default direction of filters from RADIUS.

radius-server attribute 30 original-called-number

To allow network providers to accurately match the billing function with the actual number dialed (Original Called Number (OCN)), and not the translated number to which the switch reports, use the **radius-server attribute 30 original-called-number** command in global configuration mode.

radius-server attribute 30 original-called-number

no radius-server attribute 30 original-called-number

Command Default

The *command-level defaul* t is not enabled. The translated number is sent to the NAS.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

The ITU-T Q.931 attribute is the connection control protocol of the ISDN. Some switches can send a translated dialed number identification service (DNIS) number to the network access server (NAS) instead of the OCN. These switches eventually inform the NAS about the OCN in its Q931 attribute. However, some network providers require the OCN in its Q.931 attribute.

The **radius-server attribute 30 original-called-number**command allows the OCN with its Q.931 attribute to be sent to the RADIUS Called-Station-ID, which is a check mechanism administrators use to deny or accept access from users based on the NAS (when available). This OCN is used instead of the redirected translated number reported as the DNIS by ISDN.

Examples

The following example enables the **radius-server attribute 30 original-called-number**in global configuration mode:

```
aaa new-model
radius-server attribute 30 original-called-number
```

radius-server attribute 31

To configure Calling-Station-ID (attribute 31) options, use the **radius-server attribute 31**command in global configuration mode. To disable the Calling-Station-ID (attribute 31) options, use the **no** form of this command.

radius-server attribute 31 {**append-circuit-id**| **mac format** {**default**| **ietf**| **unformatted**}| **remote-id**| **send nas-port-detail [mac-only]**}

no radius-server attribute 31 {**append-circuit-id**| **mac format** {**default**| **ietf**| **unformatted**}| **remote-id**| **send nas-port-detail [mac-only]**}

Syntax Description

append-circuit-id	Appends the PPPoE tag circuit-id and the nas-port-id to the calling-station-id.
mac format	Specifies the format of the MAC address in the Calling Station ID. Select one of the following three options: • **default** (Example: 0000.4096.3e4a) • **ietf** (Example: 00-00-40-96-3E-4A) • **unformatted** (Example: 000040963e4a)
remote-id	Sends the remote ID as the Calling Station ID in the accounting records and access requests.
send nas-port-detail	Includes all NAS port details in the Calling Station ID.
mac-only	(Optional) Includes the MAC address only, if available, in the Calling Station ID.

Command Default

The Calling-Station-ID (attribute 31) is not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The **mac format default** ,the **mac format ietf** ,the **mac format unformatted** ,and the **send nas-port-detail** [**mac-only**] keyword options were added.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

- For PPP over Ethernet over ATM (PPPoEoA) sessions:

When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

```
host.domain:vp_descr:vpi:vci
```

- For PPP over Ethernet over Ethernet (PPPoEoE) sessions:

When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

```
mac_addr
```

- For PPP over ATM sessions:

When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-ID (attribute 31) information is sent in Access and Accounting requests in the following format:

```
host.domain:vp_descr:vpi:vci
```

- For Intelligent Services Gateway RADIUS Proxy sessions:

When DHCP lease query is used, ISG RADIUS proxy recieves MAC address as well as MSISDN as the Calling-Station-ID (attribute 31) from the downstream device. Therefore, ISG RADIUS proxy must be configured to choose one of them as the Calling Station ID and send it to the ISG accounting records.

The following example shows how to specify the MAC address in the Calling Station ID to be displayed in IETF format:

```
Router(config)# radius-server attribute 31 mac format
 ietf
```

The following example shows how to allow the remote ID to be sent as the Calling Station ID:

```
Router(config)# radius-server attribute 31 remote-id
```

The following example shows how to allow the NAS port details to be included in the Calling Station ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail
```

The following example shows how to allow only the MAC address, if available, to be included in the Calling-Station-ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail mac-onl
```

Related Commands

Command	Description
radius-server attribute nas-port-id include	Uses the DHCP relay agent information option 60 and option 82 and configures the NAS-Port-ID to authenticate a user.

radius-server attribute 31 mac format

To configure a nondefault MAC address format in the calling line ID (CLID) of a DHCP accounting packet, use the **radius-server attribute 31 mac format** command in global configuration mode. To revert to the default MAC address format, use the **no** form of this command.

radius-server attribute 31 mac format {**default** | **ietf** [**lower-case** | **upper-case**] | **unformatted**}

no radius-server attribute 31 mac format {**default** | **ietf** [**lower-case** | **upper-case**] | **unformatted**}

Syntax Description

default	Sets the MAC address format to the default format (for example, aaaa.bbbb.cccc).
ietf	Sets the IETF format for MAC addresses (for example, aa-aa-bb-bb-cc-cc).
lower-case	(Optional) Sets the MAC address in IETF format in lower case.
upper-case	(Optional) Sets the MAC address in IETF format in upper case.
unformatted	Sets the unformatted raw MAC address (for example, aaaabbbbcccc).

Command Default

The MAC address format in the CLID is set to the default format.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.3(1)S	This command was modified. The **lower-case** and **upper-case** keywords were added.

Usage Guidelines

The CLID (attribute 31) carries information such as phone numbers, IP addresses, and MAC addresses.

The CLID is sent in the DHCP accounting packet only if the **radius-server attribute 31 send nas-port-detail mac-only** command is also configured along with the **radius-server attribute 31 mac format** command.

Examples

The following example shows how to set the RADIUS CLID to “unformatted”:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 31 mac format unformatted
```

The following example shows how to set the MAC address the RADIUS CLID to the IETF format in lower case:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 31 mac format ietf lower-case
```

Related Commands

Command	Description
radius-server attribute 31 send nas-port-detail mac-only	Configures CLID (attribute 31) options.

radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** command in global configuration mode. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Command Default

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the format argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server attribute 44 extend-with-addr

To add the accounting IP address before the existing session ID, use the **radius-server attribute 44 extend-with-addr** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 extend-with-addr

no radius-server attribute 44 extend-with-addr

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server attribute 44 extend-with-addr**command adds Acct-Session-Id (attribute 44) before the existing session ID (NAS-IP-Address).

When multiple network access servers (NAS) are being processed by one offload server, enable this command on all NASs and the offload server to ensure a common and unique session ID.

Note This command should be enabled only when offload servers are used.

Examples

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 extend-with-addr
```

Related Commands

Command	Description
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.
radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (accounting session ID) in access-request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req [**all** | **default-vrf** | **vrf** *vrf-name*]

no radius-server attribute 44 include-in-access-req [**all** | **default-vrf** | **vrf** *vrf-name*]

Syntax Description

all	(Optional) Enables configuration of all virtual routing and forwarding (VRF) sessions.
default-vrf	(Optional) Enables configuration of non-VRF sessions.
vrf *vrf-name*	(Optional) Enables configuration of the specified VRF session.

Command Default

RADIUS attribute 44 is not sent in access-request packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(1)DX	This command was modified. The **vrf** keyword and *vrf-name* argument were added on the Cisco 7200 series and Cisco 7401 ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)S3	This command was modified. This command was integrated into Cisco IOS Release 15.1(3)S3. The **all** and **default-vrf** keywords were added.

Usage Guidelines

The accounting session IDs may not increment uniformly and consistently; that is, between two calls, the accounting session ID can increase by more than one.

The **vrf** *vrf-name* keyword and argument specify Accounting Session IDs per VRF, which allows multiple, disjoined routing or forwarding tables, where the routes of one user have no correlation with the routes of another user.

Examples

The following example shows a configuration that sends RADIUS attribute 44 in access-request packets:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 192.0.2.3
radius-server attribute 44 include-in-access-req
```

Related Commands

Command	Description
radius-server attribute 32 include-in-access-req	Sends RADIUS attribute 32 (NAS-identifier) in an access or accounting request.
radius-server attribute 55 include-in-access-req	Sends RADIUS attribute 55 (Event-Timestamp) in accounting packets.

radius-server attribute 44 sync-with-client

To configure the offload server to synchronize accounting session information with the network access server (NAS) clients, use the **radius-server attribute 44 sync-with-client** command in global configuration mode. To disable this functionality , use the **no** form of this command.

radius-server attribute 44 sync-with-client

no radius-server attribute 44 sync-with-client

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **radius-server attribute 44 sync-with-client** command to allow the offload server to synchronize accounting session information with the NAS clients. The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted from the client to the offload server via Layer 2 Forwarding (L2F) options.

Examples

The following example shows how to configure the offload server to synchronize accounting session information with the NAS clients:

```
radius-server attribute 44 sync-with-client
```

Related Commands

Command	Description
radius-server attribute 44 extend-with-addr	Adds the accounting IP address before the existing session ID.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.

radius-server attribute 55 include-in-acct-req

To send the RADIUS attribute 55 (Event-Timestamp) in accounting packets, use the **radius-server attribute 55 include-in-acct-req** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 55 include-in-acct-req

no radius-server attribute 55 include-in-acct-req

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS attribute 55 is not sent in accounting packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 55 include-in-acct-req**command to send RADIUS attribute 55 (Event-Timestamp) in accounting packets . The Event-Timestamp attribute records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC.

Note Before the Event-Timestamp attribute can be sent in accounting packets, you >*must* configure the clock on the router. (For information on setting the clock on your router, refer to section “Performing Basic System Management” in the chapter “ System Management ” of the Cisco IOS Configuration Fundamentals and Network Management Configuration Guide .) To avoid configuring the clock on the router every time the router is reloaded, you can enable the **clock calendar-valid** command. (For information on this command, refer to the *Cisco IOS Config* uration Fundamentals and Network Management Command Reference.)

Examples

The following example shows how to enable your router to send the Event-Timestamp attribute in accounting packets. (To see whether the Event-Timestamp was successfully enabled, use the debug radiuscommand.)

```
radius-server attribute 55 include-in-acct-req
```

Related Commands

Command	Description
clock calendar-valid	Configures a system as an authoritative time source for a network based on its hardware clock (calendar).
clock set	Manually sets the system software clock.

radius-server attribute 60 include-in-access-req

To authenticate user credentials by sending a Challenge Handshake Authentication Protocol (CHAP)-Challenge (RADIUS attribute 60) in access-request packets to the RADIUS server, use the **radius-server attribute 60 include-in-access-req** command in global configuration mode. To disable this configuration, use the **no** form of this command.

radius-server attribute 60 include-in-access-req

no radius-server attribute 60 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS attribute 60 is not sent in access-request packets to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 60 include-in-access-req** command to identify the network access server (NAS) manufacturer by sending RADIUS attribute 60 (CHAP-Challenge) in an access-request. If the CHAP-Challenge value is 16 octets long, this value can either be included in the CHAP-Challenge attribute or it can be entered in the Request Authenticator field of the access-request packet.

Examples

The following example shows how to send RADIUS attribute 60 in access-request packets:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 60 include-in-access-req
Device(config)# end
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that run PPP.
aaa new-model	Enables the AAA access control model.

Command	Description
radius-server attribute 32 include-in-access-req	Sends RADIUS attribute 32 (NAS-identifier) in an access or accounting request.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (accounting session ID) in access-request packets.
radius-server attribute 55 include-in-access-req	Sends RADIUS attribute 55 (Event-Timestamp) in accounting packets.
radius-server host	Specifies a RADIUS server host.

radius-server attribute 61 extended

To enable extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61), use the **radius-server attribute 61 extended**command in global configuration mode. To disable extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61), use the **no** form of this command.

radius-server attribute 61 extended

no radius-server attribute 61 extended

Syntax Description

This command has no arguments or keywords.

Command Default

Extended attribute 61 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)XI1	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

RADIUS Attribute 61 (Network-attached storage (NAS) port-type, a number) is sent in an access-request to indicate the type of physical port of the NAS, which is authenticating the user with number.

Table 17: NAS Access Technology Values

RADIUS Value	Service Port Type
27	Wireless - IEEE 802.16
30	PPP over ATM (PPPoA)
31	PPP over Ethernet over ATM (PPPoEoA)
32	PPP over Ethernet over Ethernet (PPPoEoE)
33	PPP over Ethernet over VLAN (PPPoEoVLAN)
34	Point-to-Point Protocol over Ethernet IEEE 802.1Q Tunneling (PPPoEoQinQ)

The Value “Virtual” refers to a connection to the NAS through a transport protocol, instead of through a physical port. For example, if a user telnetted into a NAS, the value “Virtual” would be reflected as the NAS value.

There is no specific NAS value for IP sessions. The NAS value depends on the underlying transport technology values described in the table below or “Virtual” is used for IP sessions. For example, if PPP is the underlying access technology (transport protocol), the value reported is 33.

If extended attribute 61 is not enabled the following occurs:

- All PPPoA, PPPoE, PPPoEoE, PPPoEoA sessions are identified as “Virtual”.
- All PPPoEoVLAN and PPPoEoQinQ sessions are identified as VLAN.
- RFC-compliant values, such as Virtual (value 5) and Ethernet (value 15) are sent to the authentication, authorization, and accounting (AAA) records.

Examples

The following example shows how to configure global support for extended attribute 61 ports and how to specify different format e strings globally for two different types of ports:

- Type 30 (which is PPPoA)
- Type 33 (which is PPPoEoVLAN)

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended
Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUUU
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC
 type 30

Router(config)#
Router(config)# radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV
 type 33
Router(config)#
```

Related Commands

Command	Description
radius attribute nas-port-type	Configures subinterfaces such as Ethernet, VLANS, stacked VLAN (Q-in-Q), VC and VC ranges.
radius-server attribute nas-port format	Sets the NAS-Port format used for RADIUS accounting features and restores the default NAS-Port format, or sets the global attribute 61 session format e string or configures a specific service port type for attribute 61 support.

radius-server attribute 66 include-in-access-req

To identify the hostname or address of the network access server (NAS) at the initiator end of the Point-to-Point Tunneling Protocol (PPTP) tunnel by sending the Tunnel-Client-Endpoint attribute in access-request packets to the RADIUS server, use the **radius-server attribute 66 include-in-access-req** command in global configuration mode. To disable the Tunnel-Client-Endpoint attribute, use the **no** form of this command.

radius-server attribute 66 include-in-access-req

no radius-server attribute 66 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS attribute 66 is not sent in access-request packets to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

VPNs use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP or asynchronous High-Level Data Link Control [HDLC]). ISPs configure their network access servers to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel endpoint. The customer maintains IP addresses, routing, and other user database functions of the tunnel server users. Use the **radius-server attribute 66 include-in-access-req** command to identify the hostname or address of the NAS at the initiator end of the tunnel by sending RADIUS attribute 66 (Tunnel-Client-Endpoint) in an access-request packet. The tunnel information in the access-request packet allows the provider to know which PPTP service (for example, L2TP) was selected.

Examples

The following example shows a configuration that sends RADIUS attribute 66 in access-request packets:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 66 include-in-access-req
Device(config)# end
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that run PPP.
aaa new-model	Enables the AAA access control model.
radius-server attribute 67 include-in-access-req	Sends RADIUS attribute 67 (Tunnel-Server-Endpoint) in an access request.
radius-server host	Specifies a RADIUS server host.

radius-server attribute 67 include-in-access-req

To identify the hostname or address of the network access server (NAS) at the sever end of the Point-to-Point Tunneling Protocol (PPTP) tunnel by sending the Tunnel-Server-Endpoint attribute in access-request packets to the RADIUS server, use the **radius-server attribute 67 include-in-access-req** command in global configuration mode. To disable the Tunnel-Server-Endpoint attribute, use the **no** form of this command.

radius-server attribute 67 include-in-access-req

no radius-server attribute 67 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS attribute 67 is not sent in access-request packets to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

VPNs use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP or asynchronous High-Level Data Link Control [HDLC]). ISPs configure their network access servers to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel endpoint. The customer maintains IP addresses, routing, and other user database functions of the tunnel server users. Use the **radius-server attribute 67 include-in-access-req** command to specify the hostname or address of the NAS at the server end of the tunnel by sending RADIUS attribute 67 (Tunnel-Server-Endpoint) in an access-request packet. The tunnel information in the access-request packet allows the provider to know which PPTP service (for example, L2TP) was selected.

Examples

The following example shows a configuration that sends RADIUS attribute 67 in access-request packets:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 67 include-in-access-req
Device(config)# end
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that run PPP.
aaa new-model	Enables the AAA access control model.
radius-server attribute 66 include-in-access-req	Sends RADIUS attribute 66 (Tunnel-Client-Endpoint) in an access request.
radius-server host	Specifies a RADIUS server host.

radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password) , use the **radius-server attribute 69 clear** command in global configuration mode. To disable this feature and receive encrypted tunnel passwords, use the **no** form of this command.

radius-server attribute 69 clear

no radius-server attribute 69 clear

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS attribute 69 is not sent and encrypted tunnel passwords are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 69 clear**command to receive nonencrypted tunnel passwords, which are sent in RADIUS attribute 69 (Tunnel-Password). This command allows tunnel passwords to be sent in a “string” encapsulated format, rather than the standard tag/salt/string format, which enables the encrypted tunnel password.

Some RADIUS servers do not encrypt Tunnel-Password; however the current NAS (network access server) implementation will decrypt a non-encrypted password that causes authorization failures. Because nonencrypted tunnel passwords can be sent in attribute 69, the NAS will no longer decrypt tunnel passwords.

Note Once this command is enabled, all tunnel passwords received will be nonencrypted until the command is manually disabled.

Examples

The following example shows how to enable attribute 69 to receive nonencrypted tunnel passwords. (To see whether the Tunnel-Password process is successful, use the debug radius command.)

```
radius-server attribute 69 clear
```

radius-server attribute 77

To send connection speed information to the RADIUS server in the access request, use the **radius-server attribute 77** command in global configuration mode. To prevent connection speed information from being included in the access request, use the **no** form of this command.

radius-server attribute 77 {**include-in-access-req**| **include-in-acct-req**}

no radius-server attribute 77 {**include-in-access-req**| **include-in-acct-req**}

Syntax Description

include-in-access-req	Specifies that attribute 77 will be included in access requests.
include-in-acct-req	Specifies that attribute 77 will be included in accounting requests.

Command Default

RADIUS attribute 77 is sent to the RADIUS server in the access request.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)BX	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

RADIUS attribute 77 is sent to the RADIUS server in the access request by default.

RADIUS attribute 77 allows RADIUS authentication based on connection speed. Sessions can be accepted or denied based on the allowed connection speed configured for a particular user on the RADIUS server.

RADIUS attribute 77 includes the following information:

- The accounting start/stop request
- The VC class name defined with the **class-int**command
- The VC class name defined with the **class-vc** command
- The VC class name defined with the **class-range** command

The VC class name may include letters, numbers, and the characters ":" (colon), ";" (semicolon), "-" (hyphen) and "," (comma).

Examples

The following example disables the inclusion of RADIUS attribute 77 in the access request:

```
no radius-server attribute 77 include-in-access-req
```

Related Commands

Command	Description
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-range	Assigns a VC class to an ATM PVC range.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.

radius-server attribute 188 format non-standard

To send the number of remaining links in the multilink bundle in the accounting-request packet, use the radius-server attribute 188 format non-standard command in global configuration mode. To disable the sending of the number of links in the multilink bundle in the accounting-request packet, use the no form of this command.

radius-server attribute 188 format non-standard

no radius-server attribute 188 format non-standard

Syntax Description

This command has no arguments or keywords.

Command Default

RADIUS attribute 188 is not sent in accounting “start” and “stop” records.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to send attribute 188 in accounting “start” and “stop” records.

Examples

The following example shows a configuration that sends RADIUS attribute 188 in accounting-request packets:

```
radius-server attribute 188 format non-standard
```

radius-server attribute data-rate send 0

Note Effective with Cisco IOS Release 12.4, the **radius-server attribute data-rate send 0** command is not available in Cisco IOS software.

To enable the data transmit and receive rate of RADIUS server attributes 197 and 255 in accounting records, use the **radius-server attribute data-rate send 0** command in global configuration mode.

radius-server attribute data-rate send 0

no radius-server attribute data-rate send 0

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for *RADIUS server attributes 197 and 255 is* zero.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.
12.4	This command was removed.

Usage Guidelines

RADIUS attribute 197 is the Ascend-Data-Rate in an accounting-request packet. This attribute specifies the receive baud rate of the connection in bits per second over the course of the connection's lifetime.

RADIUS attribute 255 is the Ascend-Xmit-Rate in an accounting-request packet. This attribute specifies the transmit baud rate of the connection in bits per second over the course of the connection’s lifetime.

The connection is authenticated for both RADIUS attributes 197 and 255 if the following conditions are met:

- The session has ended or has failed to authenticate because the accounting-request packet has the RADIUS attribute: Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS or LOGOUT.

Note RADIUS attribute 197 does not appear in the user profile.

Examples

The following example enables the **radius-server attribute data-rate send 0 command**in global configuration mode:

```
aaa new-model
radius-server attribute data-rate send 0
```

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the **no** form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name	Name for an accept or reject list.

Command Default

List names are not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute**(server-group configuration) command, which adds attributes to an accept or reject list.

Note The list name must be the same as the list name defined in the **accounting**or **authorization**configuration command.

Examples

The following example shows how to configure the reject list "bad-list" for RADIUS authorization and accept list "usage-only" for RADIUS accounting:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# authorization reject bad-list
Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
Router(config)# radius-server host 10.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-list
Router(config-radius-attrl)# attribute 22,27-28,56-59
```

Note Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

radius-server attribute nas-port extended

The radius-server attribute nas-port extended command is replaced by the radius-server attribute nas-port format command. See the description of the radius-server attribute nas-port format command for more information.

radius-server attribute nas-port format

To set the NAS-Port format used for RADIUS accounting features and restore the default NAS-port format, or to set the global attribute 61 session format e string or configure a specific service port type for attribute 61 support, use the **radius-server attribute nas-port format** command in global configuration mode. To stop sending attribute 61 to the RADIUS server, use the **no** form of this command.

NAS-Port for RADIUS Accounting Features and Restoring Default NAS-Port Format

radius-server attribute nas-port format *format*

no radius-server attribute nas-port format *format*

Extended NAS-Port Support

radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

no radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

Syntax Description

format	NAS-Port format. Possible values for the format argument are as follows: • a--Standard NAS-Port format • b--Extended NAS-Port format • c--Carrier-based format • d--PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format • e--C onfigurable NAS-Port format
string	(Optional) Represents all of a specific port typefor format e. It is possible to specify multiple values with this argument.
type *nas-port-type*	(Optional) Allows you to globally specify different format strings to represent specific physical port types. You may set one of the extended NAS-Port-Type attribute values: • **type 30** --PPP over ATM (PPPoA) • **type 31** --PPP over Ethernet (PPPoE) over ATM (PPPoEoA) • **type 32** --PPPoE over Ethernet (PPPoEoE) • **type 33** --PPPoE over VLAN (PPPoEoVLAN) • **type 34** --PPPoE over Q-in-Q (PPPoEoQinQ)

Command Default Standard NAS-Port format for NAS-Port for RADIUS accounting features and restoring default NAS-Port format or extended NAS-Port support.

Command Modes Global configuration

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB	The PPP extended NAS-Port format was added.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q VLANs.
12.2(4)T	Format e was introduced.
12.2(11)T	Format e was extended to support PPPoX information.
12.3(3)	Format e was extended to support Session ID U.
12.3(7)XI1	Format e was extended to allow the format string to be NAS-Port-Type attribute specific. The following keyword and arguments were added: *string,* **type** *nas-port-type.*
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines The **radius-server attribute nas-port format** command configures RADIUS to change the size and format of the NAS-Port attribute field (RADIUS IETF attribute 5).

The following NAS-Port formats are supported:

- Standard NAS-Port format--This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format--The standard NAS-Port attribute field is expanded to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface that is undergoing authentication.

- Shelf-slot NAS-Port format--This 16-bit NAS-Port format supports expanded hardware models requiring shelf and slot entries.
- PPP extended NAS-Port format--This NAS-Port format uses 32 bits to indicate the interface, virtual path identifier (VPI), and virtual channel indicator (VCI) for PPPoA and PPPoEoA, and the interface and VLAN ID for PPPoE over Institute of Electrical and Electronic Engineers (IEEE) standard 802.1Q VLANs.

Format e

Before Cisco IOS Release 12.2(4)T formats a through c did not work with Cisco platforms such as the AS5400. For this reason, a configurable format e was developed. Format e requires you to explicitly define the usage of the 32 bits of attribute 25 (NAS-Port). The usage is defined with a given parser character for each NAS-Port field of interest for a given bit field. By configuring a single character in a row, such as x, only one bit is assigned to store that given value. Additional characters of the same type, such as x, will provide a larger available range of values to be stored. The table belowshows how the ranges may be expanded:

Table 18: Format e Ranges

Character	Range
x	0-1
xx	0-3
xxx	0-7
xxxx	0-F
xxxxx	0-1F

It is imperative that you know what the valid range is for a given parameter on a platform that you want to support. The Cisco IOS RADIUS client will bitmask the determined value to the maximum permissible value on the basis of configuration. Therefore, if one has a parameter that turns out to have a value of 8, but only 3 bits (xxx) are configured, 8 and 0x7 will give a result of 0. Therefore, you must always configure a sufficient number of bits to capture the value required correctly. Care must be taken to ensure that format e is configured to properly work for all NAS port types within your network environment.

The table below shows the supported parameters and their characters:

Table 19: Supported Parameters and Characters

Supported Parameters	Characters
Zero	0 (always sets a 0 to that bit)
One	1 (always sets a 0 to that bit)
DS0 shelf	f
DS0 slot	s

Supported Parameters	Characters
DS0 adaptor	a
DS0 port	p (physical port)
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L (modern line number, that is, physical terminal [TTY] number)
PPPoX slot	S
PPPoX adaptor	A
PPPoX port	P
PPPoX VLAN ID	V
PPPoX VPI	I
PPPoX VCI	C
Session ID	U

All 32 bits that represent the NAS-Port must be set to one of the above characters because this format makes no assumptions for empty fields.

Access Router

The DS0 port on a T1-based card and on a T3-based card will give different results. On T1-based cards, the physical port is equal to the virtual port (because these are the same). So, **p** and **d** will give the same information for a T1 card. However, on a T3 system, the port will give you the physical port number (because there can be more than one T3 card for a given platform). As such, **d** will give you the virtual T1 line (as per configuration on a T3 controller). On a T3 system, **p** and **d** will be different, and one should capture both to properly identify the physical device. As a working example for the Cisco AS5400, the following configuration is recommended:

```
Router (config)# radius-server attribute nas-port format e SSSSPPPPPPPPPssssppppppccccc
```

This will give one an asynchronous slot (0-16), asynchronous port (0-512), DS0 slot (0-16), DS0 physical port (0-32), DS0 virtual port (0-32), and channel (0-32). The parser has been implemented to explicitly require 32-bit support, or it will fail.

Finally, format e is supported for channel-associated signaling (CAS), PRI, and BRI-based interfaces.

Note This command replaces the **radius-server attribute nas-port extended** command.

Extended NAS-Port-Type Attribute Support

This command allows you to configure a specific service port type for extended attribute 61 support which overrides the default global setting.

Examples

In the following example, a RADIUS server is identified, and the NAS-Port field is set to the PPP extended format:

```
radius-server host 192.0.2.96 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

The following example shows how to configure global support for extended NAS-Port-Type ports and how to specify two separate format e strings globally for two different types of ports:

- type 30 (which is PPPoA)
- type 33 which is (PPPoEoVLAN)

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended
Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUUU
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC
 type 30

Router(config)#
Router(config)# radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV
 type 33
```

Related Commands

Command	Description
radius attribute nas-port-type	Configures subinterfaces such as Ethernet, vLANs, stacked VLAN (Q-in-Q), virtual circuit (VC), and VC ranges.
radius-server attribute 61 extended	Enables extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61).
vpdn aaa attribute	Enables the LNS to send PPP extended NAS-Port format values to the RADIUS server for accounting.

radius-server authorization

To set the default framed protocol in the RADIUS packet to Point-toPoint Protocol (PPP), use the **radius-server authorization**command in global configuration mode. To disable the authorization, use the **no** form of this command.

radius-server authorization default framed-protocol ppp

no radius-server authorization default framed-protocol ppp

Syntax Description

default	Specifies the default authorization action.
framed-protocol	Specifies the framed-protocol attribute type.
ppp	Specifies the service port type for the default authorization action.

Command Default

The defualt framed protocol in the RADIUS packet to PPP is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Examples

The following example shows how to set the default framed protocol in RADIUS packet to PPP:

```
Router# configure terminal
Router(config)# radius-server authorization default framed-protocol ppp
```

Related Commands

Command	Description
radius-server attribute 6	Provides for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages.

radius-server authorization missing Service-Type

The **radius-server authorization missing Service-Type** command is replaced by the **radius-server attribute 6**command. See the **radius-server attribute 6**command for more information.

radius-server backoff exponential

To configure the router for exponential backoff retransmit of accounting requests, use the **radius-server backoff exponential** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

no radius-server backoff exponential [**max-delay** *minutes*] [**backoff-retry** *retransmits*]

Syntax Description

max-delay *minutes*	(Optional) Number of retransmissions done in exponential max-delay mode. Valid range for the *minutes* argument is 1 through 120; if this option is not specified, the default value (60 minutes) will be used.
backoff-retry *retransmits*	(Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. Valid range for the *retransmits* argument is 1 through 50; if this option is not specified, the default value (5 retransmits) will be used.

Command Default

This command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced on the Cisco 6400-NRP-1, Cisco 7200 series, and Cisco 7400 series.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server backoff exponential** command is used to keep accounting records on a router for up to 24 hours. After enabling this command, the router will try to send the normal retransmissions for the number of times the *retransmits* argument is configured. Thereafter, the router will continue to retransmit accounting requests with an interval that doubles on each retransmit failure until a configured maximum interval is reached.

While the router is in "retransmit mode," it will store all accounting records that are generated during that period in its memory; the accounting records will be sent to the RADIUS server after the router comes back up before the retransmit mode is complete.

Examples

The following example shows how to configure your router for exponential backoff retransmit of accounting requests:

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

aaa accounting send stop-record authentication failure

```
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
interface BRI1/0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 0
 dialer-group 1
 isdn switch-type basic-5ess
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential
max-delay 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end
```

Related Commands

Command	Description
backoff exponential	Configures the router for exponential backoff retransmit of accounting requests per RADIUS server group.
radius-server host	Specifies a RADIUS server host.

radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** command in global configuration mode . To return to the default condition, use the **no** form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Syntax Description

This command has no arguments or keywords.

Command Default

All user responses to Access-Challenge packets are echoed to the screen.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to all users. When the **radius-server challenge-noecho** command is configured, user responses to Access-Challenge packets are not displayed unless the Prompt attribute in the user profile is set to *>echo* on the RADIUS server. The Prompt attribute in a user profile overrides the **radius-server challenge-noecho** command for the individual user. For more information, see the chapter "Configuring RADIUS" in the Cisco IOS Security Configuration Guide.

Examples

The following example stops all user responses from displaying on the screen:

```
radius-server challenge-noecho
```

radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** command in global configuration mode. To discontinue the query of the RADIUS server, use the no form of this command.

radius-server configure-nas

no radius-server configure-nas

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.

Note Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it will not take effect until you issue a **copy system:running-config nvram:startup-config** command.

Examples

The following example shows how to tell the Cisco router or access server to query the vendor-proprietary RADIUS server for already-defined static routes and IP pool definitions when the device first starts up:

```
radius-server configure-nas
```

Related Commands

Command	Description
radius-server host non-standard	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.

radius-server dead-criteria

To force one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]

no radius-server dead-criteria [**time** *seconds*| **tries** *number-of-tries*]

Syntax Description

time *seconds*	(Optional) Minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met. You can configure the time to be from 1 through 120 seconds. • If the *seconds*argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.
tries *number-of-tries*	(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100. • If the*number-of-tries*argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

Command Default

The number of seconds and number of consecutive timeouts that occur before the RADIUS server is marked as dead will vary, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelin

Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The **no** form of this command has the following cases:

- If neither the *seconds* nor the *number-of-tries* argument is specified with the **no radius-server dead-criteria**command, both time and tries will be reset to their defaults.
- If the *seconds* argument is specified using the originally set value, the time will be reset to the default value range (10 to 60).
- If the *number-of-tries* argument is specified using the originally set value, the number of tries will be reset to the default value range (10 to 100).

Examples

The following example shows how to configure the router so that it will be considered dead after 5 seconds and 4 tries:

```
Router (config)# radius-server dead-criteria time 5 tries 4
```

The following example shows how to disable the time and number-of-tries criteria that were set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria
```

The following example shows how to disable the time criterion that was set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria time 5
```

The following example shows how to disable the number-of-tries criterion that was set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria tries 4
```

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
show aaa dead-criteria	Displays dead-criteria information for a AAA server.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

radius-server deadtime

To improve RADIUS response time when some servers might be unavailable and to skip unavailable servers immediately, use the **radius-server deadtime** command in global configuration mode. To set deadtime to 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes (up to a maximum of 1440 minutes or 24 hours), for which a RADIUS server is skipped over by transaction requests.

Command Default

Dead time is set to 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the specified duration (in minutes) or unless there are no servers not marked as "dead."

Note If a RADIUS server that is marked as "dead" receives a directed-request, the directed- request is not omitted by the RADIUS server. The RADIUS server continues to process the directed-request because the request is directly sent to the RADIUS server.

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a packet is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. At at least the requisite number of retransmits plus one (for the initial transmission) have been sent consecutively across all transactions being sent to the RADIUS server without receiving a valid response from the server within the requisite timeout.

Examples

The following example specifies five minutes of deadtime for RADIUS servers that fail to respond to authentication requests:

```
radius-server deadtime 5
```

Related Commands

Command	Description
deadtime (server-group configuration)	Configures deadtime within the context of RADIUS server groups.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

radius-server directed-request

To allow users to log in to a Cisco network access server (NAS) and select a RADIUS server for authentication, use the **radius-server directed-request**command in global configuration mode. To disable the directed-request function, use the no form of this command.

radius-server directed-request [restricted]

no radius-server directed-request [restricted]

Syntax Description

restricted	(Optional) Prevents the user from being sent to a secondary server if the specified server is not available.

Command Default

The User cannot log in to a Cisco NAS and select a RADIUS server for authentication.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Note If a private RADIUS server is used as the group server by configuring the **server-private** (RADIUS) command, then the **radius-server directed-request**command cannot be configured.

The following is the sequence of events to send a message to RADIUS servers:

- If the **radius-server directed-request** command is configured:
  - A request is sent to the directed server. If there are more servers with the same IP address, the request is sent only to the first server with same IP address.

- If a response is not received, requests will be sent to all servers listed in the first method list.
- If no response is received with the first method, the request is sent to all servers listed in the second method list until the end of the method list is reached.

Note To select the directed server, search the first server group in the method list for a server with the IP address provided in a directed request. If it is not available, the first server group with the same IP address from the global pool is considered.

- Ifthe **radius-server directed-request restricted** command is configured for every server group in the method list, until the response is received from the directed server or the end of method list is reached, the following actions occur:
  - The first server with an IP address of the directed server will be used to send the request.
  - If a server with the same IP address is not found in the server group, then the first server in the global pool with the IP address of the directed-server will be used.

If the **radius-server directed-request**command is disabled using the **no radius-server directed-request** command, the entire string, both before and after the "@" symbol, is sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

If the user request has a server IP address, then the directed server forwards it to a specific server before forwarding it to the group. For example, if a user request such as user@10.0.0.1 is sent to the directed server, and if the IP address specified in this user request is the IP address of a server, the directed server forwards the user request to the specific server.

If a directed server is configured both on the server group and on the host server, and if the user request with the configured server name is sent to the directed server, the directed server forwards the user request to the host server before forwarding it to the server group. For example, if a user request of user@10.0.0.1 is sent to the directed server and 10.0.0.1 is the host server address, then the directed server forwards the user request to the host server before forwarding the request to the server group.

Note When the **no radius-server directed-request restricted** command is entered, only the restricted flag is removed, and the directed-request flag is retained. To disable the directed-request function, you must also enter the **no radius-server directed-request**command.

Examples

The following example shows how to verify that the RADIUS server is selected based on the directed request:

```
aaa new-model
aaa authentication login default radius
radius-server host 192.168.1.1
radius-server host 172.16.56.103
radius-server host 172.31.40.1
radius-server directed-request
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-mode l	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
server-private (**RADIUS**)	Configures the IP address of the private RADIUS server for the group server.

radius-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote RADIUS server, use the **radius-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

Note The **ip vrf default** command must be configured in global configuration mode before the **radius-server domain-stripping** command is configured to ensure that the default VRF name is a NULL value until the defaulf vrf name is configured.

radius-server domain-stripping [**[right-to-left]** [**prefix-delimiter** *character* [*character2 ... character7*]] [**delimiter** *character* [*character2 ... character7*]]| **strip-suffix** *suffix*] [**vrf** *vrf-name*]

no radius-server domain-stripping [**[right-to-left]** [**prefix-delimiter** *character* [*character2 ... character7*]] [**delimiter** *character* [*character2 ... character7*]]| **strip-suffix** *suffix*] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.

strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name*argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	Support was added for the **right-to-left** and **delimiter** *character*keywords and argument.
12.4(4)T	Support was added for the **strip-suffix** *suffix* and **prefix-delimiter** keywords and argument.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
XE 2.1	This command was integrated into Cisco IOS Release XE 2.1.
XE 2.5	Support was added for the **strip-suffix** *suffix* and **prefix-delimiter** keywords and argument.

Usage Guidelines

Use the **radius-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the RADIUS server. If the full username is user1@cisco.com, enabling the **radius-server domain-stripping** command results in the username “user1” being forwarded to the RADIUS server.

Use the **right-to-left**keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) would result in the username "user" being forwarded to the RADIUS server. Configuring the **right-to-left**keyword would result in the username "user@cisco.com" being forwarded to the RADIUS server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix*to specify a particular suffix to strip from usernames. For example, configuring the **radius-server domain-stripping strip-suffix cisco.net**command would result in the username user@cisco.net being stripped, while the username user@cisco.com will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **radius-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **radius-server domain-stripping s trip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter**keyword.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **radius-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]]command.
- You may configure multiple instances of the **radius-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]command with unique values for **vrf** *vrf-name*.
- You may configure multiple instances of the **radius-server domain-stripping strip-suffix** *suffix*[**vrf** *per-vrf*]command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **radius-server domain-stripping**command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username

“cisco/user@cisco.com” will be forwarded to the RADIUS server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
radius-server domain-stripping right-to-left delimiter @\$
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username “user@cisco.com” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com#cisco.com, the username “user@cisco.com” will be forwarded.

```
radius-server domain-stripping prefix-delimiter / delimiter $@#
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username “cisco/user@cisco.net” will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
tacacs-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the TACACS+ server.

radius-server extended-portnames

The **radius-server extended-portnames** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server host

Note The **radius-server host** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* command. For more information about the **radius server** command, see Cisco IOS Security Command Reference: Commands M to R.

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

Cisco IOS Release 12.4T and Later Releases

radius-server host {*hostname*| *ip-address*} [**alias** {*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

All Other Releases

radius-server host {*hostname*| *ip-address*} [**alias** {*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**test username** *user-name* **[ignore-acct-port] [ignore-auth-port]** [**idle-time** *minutes*]] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii**| **hex**}]| **pac**] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
acct-port *port-number*	(Optional) UDP destination port for accounting requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1646.

auth-port *port-number*	(Optional) UDP destination port for authentication requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1645.
non-standard	Parses attributes that violate the RADIUS standard.
timeout *seconds*	(Optional) Time interval (in seconds) that the device waits for the RADIUS server to reply before retransmitting. • The timeout keyword overrides the global value of the **radius-server timeout** command. • If no timeout value is specified, a global value is used; the range is from 1 to 1000.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or there is a delay in responding. • The retransmit keyword overrides the global setting of the **radius-server retransmit** command. • If no retransmit value is specified, a global value is used; the range is from 1 to 100.
test username *user-name*	(Optional) Sets the test username for the automated testing feature for RADIUS server load balancing.
ignore-acct-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the accounting port.
ignore-auth-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the authentication port.
idle-time *minutes*	(Optional) Length of time (in minutes) the server remains idle before it is quarantined and test packets are sent out. The range is from 1 to 35791. The default is 60.
backoff exponential	(Optional) Sets the exponential retransmits backup mode.

max-delay *minutes*	(Optional) Sets the maximum delay (in minutes) between retransmits. • **max-delay** *minutes* *minutes*—The range is from 1 to 120. The default value is 3.
key-wrap encryption-key	(Optional) Specifies the key-wrap encryption key.
message-auth-code-key	Specifies the key-wrap message authentication code key.
format	(Optional) Specifies the format of the message authenticator code key. • Valid values are: ◦ **ascii**—Configures the key in ASCII format. ◦ **hex**—Configures the key in hexadecimal format.
backoff-retry *number-of-retransmits*	(Optional) Specifies the exponential backoff retry. • *number-of-retransmits*—Number of backoff retries. The range is from 1 to 50. The default value is 8.
pac	(Optional) Generates the per-server Protected Access Credential (PAC) key.
key	(Optional) Encryption key used between the device and the RADIUS daemon running on this RADIUS server. • The **key** keyword overrides the global setting of the **radius-server key** command. If no key string is specified, a global value is used. **Note** The **key** keyword is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

encryption-key	Specifies the encryption key. • Valid values for *encryption-key* are: ◦ **0**—Specifies that an unencrypted key follows. ◦ **7**—Specifies that a hidden key follows. ◦ String specifying the unencrypted (clear-text) server key.

Command Default No RADIUS host is specified and RADIUS server load balancing automated testing is disabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	This command was modified. The **alias** keyword was added.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B. The **backoff exponential**, **backoff-retry**, **key**, and **max-delay** keywords and *number-of-retransmits, encryption-key*, and *minutes* arguments were added.
12.2(28)SB	This command was integrated into Cisco release 12.2(28)SB. The **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds* keywords and arguments were added for configuring the RADIUS server load balancing automated testing functionality.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was modified. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.

Release	Modification
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(1)S	This command was modified. The **key-wrap encryption-key**, **message-auth-code-key**, **format**, **ascii**, and **hex** keywords were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was deprecated in Cisco IOS Release 15.4(2)S.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

We recommend the use of a test user who is not defined on the RADIUS server for the automated testing of the RADIUS server. This is to protect against security issues that can arise if the test user is not configured correctly.

If you configure one RADIUS server with a nonstandard option and another RADIUS server without the nonstandard option, the RADIUS server host with the nonstandard option does not accept a predefined host. However, if you configure the same RADIUS server host IP address for different UDP destination ports, where one UDP destination port (for accounting requests) is configured using the **acct-port** keyword and another UDP destination port (for authentication requests) is configured using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option. This results in resetting all the port numbers. You must specify a host and configure accounting and authentication ports on a single line.

To use separate servers for accounting and authentication, use the zero port value as appropriate.

RADIUS Server Automated Testing

When you use the **radius-server host** command to enable automated testing for RADIUS server load balancing:

- The authentication port is enabled by default. If the port number is not specified, the default port number (1645) is used. To disable the authentication port, specify the **ignore-auth-port** keyword.
- The accounting port is enabled by default. If the port number is not specified, the default port number (1645) is used. To disable the accounting port, specify the **ignore-acct-port** keyword.

Examples

The following example shows how to specify host1 as the RADIUS server and to use default ports for both accounting and authentication depending on the Cisco release that you are using:

```
radius-server host host1
```

The following example shows how to specify port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example shows how to specify the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to six, sets the retransmit value to five, and sets "rad123" as the encryption key, thereby matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example shows how to specify the RADIUS server host1 for accounting but not for authentication, and the RADIUS server host2 for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example shows how to specify four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for three retries and the timeout is configured for five seconds; that is, the RADIUS request will be transmitted three times with a delay of five seconds. Thereafter, the device will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The device will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

The **pac** keyword allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC's peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

The following example shows how to configure automatic PAC provisioning on a device. In seed devices, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Examples

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified depending on the Cisco release that you are using:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces that run PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.

Command	Description
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are to be selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies the number of times Cisco software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval that a device waits for a server host to reply.
test aaa group	Tests the RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard**command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

radius-server host {*host-name*| *ip-address*} **non-standard**

no radius-server host {*host-name*| *ip-address*} **non-standard**

Syntax Description

host-name	DNS name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.

Command Default

No RADIUS host is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **radius-server host non-standard** command enables you to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard**command.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*.

Examples

The following example specifies a vendor-proprietary RADIUS server host named *alcatraz*:

```
radius-server host alcatraz non-standard
```

Related Commands

Command	Description
radius-server configure-nas	Allows the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up.
radius-server host	Specifies a RADIUS server host.

radius-server key

Note The **radius-server key** command is deprecated from Cisco IOS Release 15.4(2)S. To configure an IPv4 or IPv6 RADIUS server, use the **radius server** *name* **key** command. For more information about the **key (config-radius-server)** command, see *Cisco IOS Security Command Reference: Commands D to L*.

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

radius-server key {**0** *string*| **7** *string*} *string*

no radius-server key

Syntax Description

0 *string*	Specifies that an unencrypted key follows. The unencrypted (cleartext) shared key.
7 *string*	Specifies that a hidden key follows. The hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	This command was modified. The *string* argument was modified as follows: • **0** *string* • **7** *string* • *string*
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.4(2)S	This command was deprecated in Cisco IOS Release 15.4(2)S.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “key1”:

```
Device(config)# radius-server key key1
```

The following example sets the authentication and encryption key to “anykey.” The 7 specifies that a hidden key will follow.

```
service password-encryption
radius-server key 7 anykey
```

After you save your configuration and use the show-running config command, an encrypted key will be displayed as follows:

```
Device# show running-config
!
!
 radius-server key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables AAA access control model.

Command	Description
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
service password-encryption	Encrypt passwords.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server load-balance

To enable RADIUS server load balancing for the global RADIUS server group referred to as “radius” in the authentication, authorization and accounting (AAA) method lists, use the radius-server load-balance command in global configuration mode. To disable RADIUS server load balancing, use the **no** form of this command.

radius-server load-balance method least-outstanding [**batch-size** *number*] **[ignore-preferred-server]**

no radius-server load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1-2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single AAA session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Default

If this command is not configured, global RADIUS server load balancing will not occur.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples The following example shows how to enable load balancing for global RADIUS server groups. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information. You can use the delimiting characters to display only the relevant parts of the configuration.

Examples The following shows the relevant RADIUS configuration:

```
Router# show running-config | inc radius
aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa authentication ppp**command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the keyword start-stop.
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption key identified.
- The **radius-server load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.

Examples The debug output below shows the selection of preferred server and processing of requests for the configuration above.

```
Router# show debug
General OS:
  AAA server group server selection debugging is on
Router#
<sending 10 pppoe requests>
Router#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(0000001A):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001A):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001D):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server
.
.
.
```

Server Status Information for Global RADIUS Server Group Example

The output below shows the AAA server status for the global RADIUS server group configuration example.

```
Router# show aaa server
RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
```

```
            Transaction:success 5, failure 0
     Author:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Account:request 5, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 3247ms
            Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
Router#
```

The output shows the status of two RADIUS servers. Both servers are up and, in the last 2 minutes, have processed successfully:

- 5 out of 6 authentication requests
- 5 out of 5 accounting requests

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
test aaa group	Tests RADIUS load balancing server response manually.

radius-server local

To enable the access point or wireless-aware router as a local authentication server and to enter into configuration mode for the authenticator, use the **radius-server local**command in global configuration mode. To remove the local RADIUS server configuration from the router or access point, use the **no**form of this command.

radius-server local

no radius-server local

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that the access point is being configured to serve as a local authentication server:

```
Router(config)# radius-server local
```

Usage Guidelines

This command is not supported on bridges.

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

radius local-server pac-generate expiry

To specify the encryption of the expiration time (expiry) and password for the Protected Access Credentials (PAC) in the RADIUS local server, use the **radius local-server pac-generate expiry**command in privileged EXEC mode.

radius local-server pac-generate expiry *filename* [**password** *string*] [**expiry** *days*]

Syntax Description

filename	Filename to save the generated PAC.
password *string*	(Optional) Specifies to encrypt the PAC password and the password to be encrypted.
expiry *days*	(Optional) Specifies to encrypt the expiry time of the generated PAC and the number of days. The range is from 1 to 4095. Default is one day.

Command Default

The expiry encryption for PAC in the RADIUS local server is one day.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the router to expire the “user.pac” file in two days:

```
Router# radius local-server pac-generate expiry user.pac expiry 2
```

Related Commands

Command	Description
show radius local-server statistics	Displays the statistics for the local authentication server.

radius-server optional-passwords

To specify that the first RADIUS request to a RADIUS server be made >*without* password verification, use the **radius-server optional-passwords** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server optional-passwords

no radius-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Examples

The following example configures the first login to not require RADIUS verification:

```
radius-server optional-passwords
```

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The range is 0 to 100.

Command Default

The default number of retransmission attempts is 3.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server retransmit rate to 5.

Examples

The following example shows how to specify a retransmit counter value of five times:

```
Router(config)# radius-server retransmit 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server retry method reorder

To specify the reordering of RADIUS traffic retries among a server group, use the radius-server retry method reorder command in global configuration mode. To disable the reordering of retries among the server group, use the **no** form of this command.

radius-server retry method reorder

no radius-server retry method reorder

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, RADIUS traffic is not reordered among the server group.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use this command to reorder RADIUS traffic to another server in the server group when the first server fails in periods of high load. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic will not be automatically switched back to the first server.

If the **radius-server retry method reorder**command is not configured, each RADIUS server is used until marked dead. The nondead server that is closest to the beginning of the list is used for the first transmission of a transaction and for the configured number of retransmissions. Each nondead server in the list is thereafter tried in turn.

Examples

The following example shows that RADIUS server retry has been configured:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 192.2.3.4 key rad123
```
radius-server host 192.5.6.7 key rad123

Related Commands

Command	Description
radius-server transaction max-tries	Specifies the maximum number of transmissions that may be retried per transaction on a RADIUS server.

radius-server source-ports extended

To enable 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests, use the **radius-server source-ports extended** command in global configuration mode. To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

radius-server source-ports extended

no radius-server source-ports extended

Syntax Description

This command has no arguments or keywords.

Command Default

Ports 1645 and 1646 are used as the source ports for RADIUS requests.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The identifier field of the RADIUS packet is 8 bits long, and yields 256 unique identifiers. A NAS uses one port (1645) as the source port to send out access requests to the RADIUS server and one port (1646) as the source port to send out accounting requests to the RADIUS server. This scheme allows for 256 outstanding access requests and 256 outstanding accounting requests.

If the number of outstanding access requests or accounting requests exceeds 256, the port and ID space will wrap, and all subsequent RADIUS requests will be forced to reuse ports and IDs that are already in use. When the RADIUS server receives a request that uses a port and ID that is already in use, it treats the request as a duplicate. The RADIUS server then drops the request.

The **radius-server source-ports extended** command allows you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

Examples

The following example shows how to configure a NAS to use 200 ports in the range from 21645 to 21844 as the source ports for RADIUS requests:

```
Router(config)# radius-server source-ports extended
```

radius-server throttle

To configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **radius-server throttle**command in global configuration mode. To disable throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **no** form of this command.

radius-server throttle [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]

no radius-server throttle [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]

Syntax Description

accounting *threshold*	Configures the threshold value for accounting requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access *threshold*	Configures the threshold value for access requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access-timeout *number-of-timeouts*	(Optional) Specifies the number of consecutive access timeouts that are allowed before the access request is dropped. The range is 1 through 10. The default value is 3.

Command Default

Throttling is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was implemented on the Cisco 10,000 series routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

Examples

The following examples show how to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

The following example shows how to limit the number of accounting requests sent to a RADIUS server to 100:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle accounting 100
```

The following example shows how to limit the number of access request packets sent to a RADIUS server to 200 and sets the number of timeouts allowed per transactions to 2:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle access 200
Router(config)# radius-server throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle accounting 100 access 200
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Specifies the number of seconds a router waits for a server host to reply before timing out.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
throttle	Configures server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

radius-server timeout

To set the interval for which a router waits for a server host to reply, use the **radius-server timeout** command in global configuration mode. To restore the default, use the **no**form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. The range is 1 to 1000. The default is 5 seconds .

Command Default

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set the number of seconds a router waits for a server host to reply before timing out.

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server timeout to 15 seconds.

Examples

The following example shows how to set the interval timer to 10 seconds:

```
radius-server timeout 10
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.

Command	Description
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server transaction max-tries

To specify the maximum number of transmissions that may be retried per transaction on a RADIUS server, use the radius-server transaction max-retries command in global configuration mode. To disable the number of retries that were configured, use the **no** form of this command.

radius-server transaction max-tries *number*

no radius-server transaction max-tries *number*

Syntax Description

number	Total number of transmissions per transaction. The default is eight.

Command Default

Eight transmissions

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use this command to specify the maximum number of transmissions that may be retried per transaction on a RADIUS server. This command has no meaning if the **radius-server retry method order** command has not been already configured.

Examples

The following example shows that a RADIUS server has been configured for six retries per transaction:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 192.2.3.4
radius-server host 192.6.7.8
```

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.

radius-server unique-ident

To enable the acct-session-id-count variable containing the unique identifier variable, use the **radius-server unique-ident**command in global configuration mode. To disable the acct-session-id-count variable, use the **no** form of this command.

radius-server unique-ident *id*

no radius-server unique-ident

Syntax Description

id	Unique identifier represented by the first eight bits of the acct-session-id-count variable. Valid values range from 0 to 255.

Command Default

The acct-session-id-count variable is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **radius-server unique-ident**command to increase the size of the accounting session identifier (ID) variable from 32 bits to 56 bits.

RADIUS attribute 44, Accounting Session ID, is a unique accounting identifier that makes it easy to match start and stop records in a log file. Accounting session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

The acct-session-id variable is a 32-bit variable that can take on values from 00000000-FFFFFFFF.

The acct-session-id-count variable enabled by the **radius-server unique-ident**command is a 32-bit variable. The first eight bits of the variable are reserved for the unique identifier, an identifier that allows the RADIUS server to identify an accounting session if a reload occurs. The remaining 24 bits of the acct-session-id-count variable acts as a counter variable. When the first acct-session-id variable is assigned, the acct-session-id-count variable is set to 1. The acct-session-id-count variable increments by one every time the acct-session-id variable wraps.

The acct-session-id-count variable can take on values from ##000000-##FFFFFF, where ## represents the eight bits that are reserved for the unique identifier variable.

The acct-session-id-count and acct-session-id variables are concatenated before being sent to the RADIUS server, resulting in the accounting session being represented by the following 56-bit variable:

##000000 00000000-##FFFFFF FFFFFFFF

Examples

The following example shows how to enable the acct-session-id-count variable and sets the unique identifier variable to 5:

```
radius-server unique-ident 5
```

radius-server vsa disallow unknown

To configure the IOS to deny access when the RADIUS server returns unknown Vendor-Specific Attributes (VSAs) in its Access-Accept attribute, use the **radius-server vsa disallow unknown** command in global configuration mode.

To permit access when the RADIUS server sends unknown VSAs, use the **no** form of this command.

radius-server vsa disallow unknown

no radius-server vsa disallow unknown

Command Default

Not enabled

Command Modes

Global configuration: Router(config)#

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

It is suggested that unknown VSAs should be ignored by RADIUS clients. If an Access-Accept attribute is received that includes an attribute of unknown type, then a RADIUS client can assume that it is a potential service definition, and treat it as an Access-Reject attribute. However, there may be interoperability issues with the above suggestion, and this is why the **no** form of this command may be used in certain scenarios to configure the IOS to permit access when the RADIUS server sends unknown VSAs.

Related Commands

Command	Description
radius-server vsa send	Configures the network access server (NAS) to recognize and use VSAs.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), use the **radius-server vsa send** command in global configuration mode. To disable the NAS from using VSAs, use the **no** form of this command.

radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] **[3gpp2]**

no radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] **[3gpp2]**

Syntax Description

accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Returns the Cisco NAS port VSA. **Note** Due to the IETF requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is obsoleted by default.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3GPP2) Cisco VSAs to the 3GPP2 packet type.

Command Default

NAS is not configured to recognize and use VSAs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRA	This command was modified. The **cisco-nas-port** and **3gpp2** keywords were added to provide backward compatibility for Cisco VSAs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Release	Modification
Cisco IOS XE Release 3.8S	This command was modified. The **accounting** and **authentication** keywords were enabled by default for NAS to use VSAs in accounting and authentication requests, respectively.

Usage Guidelines

The IETF draft standard specifies a method for communicating vendor-specific information between the NAS and the RADIUS server by using the VSA (attribute 26). VSAs allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send** command enables the NAS to recognize and use both accounting and authentication VSAs. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to accounting attributes only. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to authentication attributes only. Use the **show running-config all** command to see the default **radius-server vsa send accounting** and **radius-server vsa send authentication** commands.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named cisco-avpair. The value is a string with the following format:

```
"protocol : attribute separator value"
```

In the preceding example, *protocol* is a value of the Cisco protocol attribute for a particular type of authorization; *attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification; and *separator* is = for mandatory attributes. This solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Multiple Named IP Address Pools feature to be activated during IP authorization (that is, during the PPP Internet Protocol Control Protocol [IPCP] address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a NAS Prompt user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, see RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example shows how to configure the NAS to recognize and use vendor-specific accounting attributes:

```
Device(config)# radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-Port attribute with RADIUS IETF attribute 26 and displays extended field information.
show running-config all	Displays complete configuration information, including the default settings and values.

rate-limit (firewall)

To limit the number of Layer 7 Session Initiation Protocol (SIP) or H.323 protocol messages that strike the Cisco IOS firewall every second, use the **rate-limit** command in policy-map-class configuration mode. To remove the rate limit from the configuration, use the **no** form of this command.

rate-limit *limit-number*

no rate-limit *limit-number*

Syntax Description

limit-number	Number of application messages allowed per second. Range: 1 to 2147483647.

Command Default

No rate limit is configured.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	Support for the H.323 protocol was introduced.

Usage Guidelines

Use this command when configuring a rate-limiting mechanism to monitor the call attempt rate and the number of calls per second for the H.323 or SIP protocol.

The rate-limit command is used with the policy-map type inspect command and must be configured with the class type inspect command.

When configuring a rate-limiting mechanism for the H.323 or SIP protocol, the rate-limit command is used with the appropriate match command to choose the required control messages. For the H.323 protocol, the rate limit command is used with the match message command. For the SIP protocol, the rate limit command is used with the match request command.

Examples

The following example configures a rate limiting mechanism of 5 invite messages per second for the SIP class map "my_sip_rt_msgs":

```
class-map type inspect sip match-any my_sip_rt_msgs
 match request method invite
 policy-map type inspect sip my_sip_policy
 class type inspect sip my_sip_rt_msgs
 rate-limit 5
```

The following example configures a rate-limiting mechanism of 16 setup messages per second to monitor the call attempt rate for H.323 protocol based calls:

```
class-map type inspect h323 match-any my_h323_rt_msgs
 match message setup
 policy-map type inspect h323 my_h323_policy
 class type inspect h323 my_h323_rt_msgs
 rate-limit 16
```

Related Commands

Command	Description
class type inspect	Specifies the class on which an action is to be performed.
match message	Configures the match criterion for a class map on the basis of H.323 protocol messages.
policy-map type inspect	Creates an inspect type policy map.

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd**command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*

no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related--Composed of an autonomous system number and an arbitrary number.
- IP-address-related--Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit autonomous-system-number **:** *your 32-bit number* For example, 101:3.

32-bit IP address **:** *your 16-bit number* For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

reauthentication time through rsa-pubkey

reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time**command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

reauthentication time *seconds*

no reauthentication time *seconds*

Syntax Description

seconds	Number of seconds after which reauthentication occurs. Range is from 1 to 4294967295. Default is 0.

Command Default

0 seconds, which means group members are not required to reauthenticate.

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
Router(config-radsrv-group)# reauthentication time 30
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.

Command	Description
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

reconnect

To enable Internet Key Exchange Version 2 (IKEv2) support for the Cisco AnyConnect Reconnect feature, use the **reconnect** command in IKEv2 profile configuration mode. To disable IKEv2 reconnect, use the **no** form of this command.

reconnect [**timeout** *seconds*]

no reconnect

Syntax Description

timeout *seconds*	(Optional) Interval, in seconds. The range is from 600 to 86400. The default is 1800.

Command Default

The IKEv2 reconnect is disabled.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

The Auto Reconnect feature in the Cisco AnyConnect client helps the Cisco AnyConnect VPN client to remember the session for a period of time and to resume the connection when a network goes down or a client drops out of network after establishing the secure channel. As AnyConnect Client is extensively used with IKEv2, IKEv2 extends the Auto Reconnect feature support on IOS through the IOS IKEv2 support for Auto Reconnect feature of AnyConnect feature.

Examples

The following example shows how to configure an IKEv2 profile with a reconnect interval of 900 seconds:

```
Device(config)# crypto ikev2 profile profile2
Device(config-ikev2-profile)# reconnect 900
```

Related Commands

Command	Description
crypto ikev2 profile	Configures an IKEv2 profile.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect**command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url url

no redirect url url

Syntax Description

url	URL to which clients should be redirected.
url	Valid URL.

Command Default

No default behavior or values

Command Modes

Identity policy configuration (config-identity-policy)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples

The following example shows the URL to which clients are redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.example.com
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

redirect gateway

To configure an Internet Key Exchange Version 2 (IKEv2) redirect mechanism on a gateway for specific profiles, use the **redirect gateway** command in IKEv2 profile configuration mode. To remove the redirects mechanism, use the **no** form of this command.

redirect gateway auth

no redirect gateway

Syntax Description

auth	Enables the redirects mechanism on the gateway upon security association (SA) authentication.

Command Default

The redirects mechanism is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.2(4)M	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to enable the redirect mechanism on the gateway when authenticating an SA for specific IKEv2 profiles.

A thorough security analysis shows that redirect during IKE_AUTH is neither more nor less secure than redirect during IKE_INIT. However, for performance and scalability reasons, we recommend redirect during IKE_INIT.

Examples

The following example shows how to enable the redirects mechanism:

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 profile prof1
Device(config-ikev2-profile)# redirect gateway auth
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

redundancy (cs-server)

To specify that the active certificate server (CS) is synchronized to the standby CS, use the **redundancy** command in certificate server configuration mode. To return to the default, use the **no** version of this command.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Redundancy is not configured for the certificate server.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Use the **redundancy** command only if the your router has redundant capabilities for an active and standby CS.

Examples

```
Router(config)#crypto pki server CA
Router(cs-server)#redundancy
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials

Command	Description
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.

Command	Description
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

redundancy (firewall)

To enable firewall high availability (HA), use the redundancy command in parameter-map type inspect configuration mode. To disable the firewall, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

The firewall is disabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Examples

```
Device>configure terminal
Device(config)#parameter-map type inspect global
Device(config-profile)# redundancy
```

Related Commands

Command	Description
parameter-map type inspect global	Configures a global parameter map.

redundancy (GDOI)

To enable Group Domain of Interpretation (GDOI) redundancy configuration mode and to allow for key server redundancy, use the **redundancy** command in GDOI local server configuration mode. To disable GDOI redundancy, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Key server redundancy is not supported for a key server.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command must be configured before configuring related redundancy commands, such as for key server peers, local priority, and timer values. Use the **local priority** command to set the local key server priority. Use the **peer address ipv4**command to configure the peer address that belongs to the redundancy key server group.

Examples

The following example shows that key server redundancy has been configured:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.

Command	Description
peer address ipv4	Configures the peer key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

redundancy asymmetric-routing enable

To establish an asymmetric flow diversion tunnel for each redundancy group, use the **redundancy asymmetric-routing enable** command in interface configuration mode. To remove the established flow diversion tunnel, use the **no** form of this command.

redundancy asymmetric-routing enable

no redundancy asymmetric-routing enable

Syntax Description

This command has no arguments or keywords.

Command Default

An asymmetric routing traffic diversion tunnel is not configured for redundancy groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

You must configure this command on a traffic interface that sends or receives asymmetric routing traffic. A tunnel is established between the traffic interface and the asymmetric routing interface for each redundancy group.

Examples

The following example shows how to enable redundancy group asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# redundancy asymmetric-routing enable
```

Related Commands

Command	Description
asymmetric-routing	Sets up an asymmetric routing link interface and enables applications to divert packets received on the standby redundancy group to the active.
interface	Configures an interface and enters interface configuration mode.

redundancy group

To configure fault tolerance for the mobile router, use the **redundancy group** command in mobile router configuration mode. To disable this functionality, use the **no** form of this command.

redundancy group *name*

no redundancy group *name*

Syntax Description

name	Name of the mobile router group.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **redundancy group** command provides f ault tolerance by selecting one mobile router in the redundancy group *name* argument to provide connectivity for the mobile networks. This mobile router is in the active state. The other mobile routers are passive and wait until the active mobile router fails before a new active mobile router is selected. Only the active mobile router registers and sets up proper routing for the mobile networks. The redundancy state is either active or passive.

Examples

The following example selects the mobile router in the sanjose group, to provide fault tolerance:

```
ip mobile router
 redundancy group sanjose
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
standby name	Configures the name of the standby group, which is associated with the mobile router.

redundancy group (interface)

To enable the redundancy group (RG) traffic interface configuration, use the **redundancy group** command in interface configuration mode. To remove the redundancy group traffic interface configuration, use the **no** form of this command.

redundancy group *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}| **autoconfig**} [**exclusive**] [**decrement** *value*]

no redundancy group *id* {**ip**| **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}}

Syntax Description

id	Redundancy group ID. Valid values are from 1 and 2.
ip *virtual-ip*	Enables IPv4 RGs and sets a virtual IPv4 address.
ipv6	Enables IPv6 RGs.
link-local-address	Link local address.
ipv6-address/*prefix-length*	IPv6 address and the length of the IPv6 prefix. IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
autoconfig	Obtains IP addresses through autoconfiguration.
exclusive	(Optional) Specifies whether the interface is exclusive to an RG.
decrement *number*	(Optional) Specifies the number that is decremented from the priority when the state of an interface goes down. The configured decrement value overrides the default number that is configured for an RG. Valid values are from 1 to 255.

Command Default

Redundancy group traffic interface configuration is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. The *virtual-ip*, *link-local-address*, *ipv6-address*/*prefix-length* arguments and **ip**, **ipv6**, and **autoconfig** keywords were added.

Usage Guidelines

Use this command to configure a redundancy group for stateful switchover.

The virtual IP address and the physical address must be in the same subnet.

When autoconfiguration is enabled, the interface obtains an IP address automatically.

Examples

The following example shows how to enable the IPv6 redundancy group traffic interface configuration:

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# redundancy group 2 ipv6 FE80::260:3EFF:FE11:6770 exclusive
```

Related Commands

Command	Description
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
interface	Configures an interface and enters interface configuration mode.
name	Configures the name of a redundancy group.
preempt	Enables preemption on a redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures an RII for a redundancy group.

redundancy inter-device

To enter inter-device configuration mode, use the **redundancy inter-device** command in global configuration mode. To exit inter-device configuration mode, use the **exit** command. To remove all inter-device configuration, use the no form of this command.

redundancy inter-device

no redundancy inter-device

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not enabled, you cannot configure stateful failover for IPSec.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Note

- Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.
- If the **redundancy inter-device** command is configured on the device, and IPSec is configured for stateful failover, IPSec would expect SSO configuration to be complete and would send SA requests only if the device becomes active. If IPSec stateful failover is not needed, then **redundancy inter-device** need not be configured on the device.

Use the **redundancy inter-device** command to enter inter-device configuration mode, which allows you to enable and protect Stateful Switchover (SSO) traffic.

Examples

The following example shows how to issue the **redundancy inter-device** command when enabling SSO:

```
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
```

```
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
!
```

The following example shows how to issue the **redundancy inter-device** command when configuring SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the redundant peer.
local-port	Defines the local SCTP that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.
scheme	Defines that redundancy scheme that is used between two devices.

redundancy rii

To configure the redundancy interface identifier (RII) for redundancy group protected traffic interfaces, use the **redundancy rii** command in interface configuration mode. To remove the redundant interface from the redundancy group, use the **no** form of this command.

redundancy rii *id* [**decrement** *number*]

no redundancy rii

Syntax Description

id	Redundancy interface identifier. The range is from 1 to 65535.
decrement *number*	(Optional) Specifies the decrement value. When the redundant interface is down, the run-time priority of all redundancy groups configured on the router will be decremented. Valid values are from 1 to 255.

Command Default

RII is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T. The **decrement** *number* keyword-argument pair was added.

Usage Guidelin

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Every interface associated with one or more redundancy groups must have a unique RII assigned to it. The RII allows interfaces to have a one-to-one mapping between peers.

Examples

The following example shows how to configure the RII for Gigabit Ethernet interface 0/0/0:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# redundancy rii 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy group	Enables redundancy group redundancy traffic interface configuration.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancy stateful**command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**

no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Command Default

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **redundancy stateful**command uses an existing IPSec profile (which is specified via the **crypto ipsec profile**command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
```

```
ip address 209.165.201.1 255.255.255.224
standby 1 ip 209.165.201.3
standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description

This command has no arguments or keywords.

Command Default

Key rollover is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the certification authority (CA). When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”.

```
crypto ca trustpoint trustme2
 enrollment url
http://
trustme2
```

```
.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 regenerate
 password revokeme
 rsakeypair trustme2 2048
 exit
crypto ca authenticate trustme2
crypto ca enroll trustme2
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

regexp (profile map configuration)

To create an entry in a cache profile group that allows authentication and authorization matches based on a regular expression, use the **regexp** command in profile map configuration mode. To disable a regular expression entry, use the **no** form of this command.

regexp *matchexpression* {**any**| **only**} **[no-auth]**

no regexp *matchexpression* {**any**| **only**}

Syntax Description

matchexpression	String representing a regular expression on which to match.
any	Specifies that any unique instance of a AAA server response that matches the regular expression is saved in the cache.
only	Specifies that only one instance of a AAA server response that matches the regular expression is saved in the cache.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No regular expression entries are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to create an entry in a cache profile group that matches based on a regular expression, such as .*@example.com or .*@xyz.com.

Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.

Examples

The following example creates an entry in the cache profile group networkusers that authorizes network access to any example company user. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa cache profile networkusers
Router(config-profile-map)# regexp .*@example.com any no-auth
```

Related Commands

Command	Description
profile	Creates an individual authentication and authorization cache profile based on an exact username match.

registration interface

To specify the interface to be used for a Group Domain of Interpretation (GDOI) registration, use the **registration interface** command in GDOI local server configuration mode. To disable an interface, use the **no** form of this command.

registration interface *type slot/port*

noregistration interface *type slot/port*

Syntax Description

type	Type of interface (see the table below).
slot /port	Slot and port number of the interface.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The table below lists the types of interface that may be used for the *type* argument.

Table 20: Type of Interface

Interface	Description
Async	Async interface
BVI	Bridge-Group Virtual Interface
CDMA-1x	Code division multiple access 1x interface
CTunnel	CTunnel interface
Dialer	Dialer interface
Ethernet	Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3

Interface	Description
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink group interface
Null	Null interface
Serial	Serial
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual Template interface
Virtual-TokenRing	Virtual TokenRing

Examples

The following example shows that the interface is Ethernet 0/0:

```
registration interface Ethernet 0/0
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

registration periodic crl trustpoint

To enable periodic registrations for the Group Domain of Interpretation (GDOI) key server (KS) when new certificate revocation lists (CRLs) become available for the configured public key infrastructure (PKI) trustpoint certificate authority (CA), use the **registration periodic crl trustpoint** command in GDOI local server configuration mode. To disable the registration, use the **no** form of this command.

registration periodic crl trustpoint *trustpoint-name*

no registration periodic crl trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Name of the PKI trustpoint CA.

Command Default

Periodic registrations are not enabled.

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Examples

The following example enables the GET VPN CRL Checking feature on KSs:

```
crypto gdoi group gdoi_group1
 Server local
  registration periodic crl trustpoint mycert
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group.
server local	Designates a device as a GDOI key server.

registration retry count

To configure the number of times that a Transitory Messaging Services (TMS) registration message is sent to a controller, use the **registration retry count** command in parameter-map configuration mode. To configure the consumer to use the default registration retry count value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **registration retry count** command is not available in Cisco IOS software.

registration retry count *number*

no registration retry count *number*

Syntax Description

number	Number of times that a registration message is retransmitted. A number from 1 through 5 is entered.

Command Default

The following default value is used if this command is not configured or if the **no** form is entered: 3

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **registration retry count** command is entered on a consumer to configure the number of times that an implicit registration request message is transmitted.

The consumer must register with the controller before the controller can send Control Information Messages (CIMs). Implicit registration requests are automatically sent to the controller when a TMS type service policy is activated on the consumer.

By default, a consumer sends a registration request message to the controller once every 3 minutes for up to three times or until successfully registered. If the consumer is a member of multiple groups, it sends a separate registration request messages to the controller of each group.

Note Explicit registration is configured by entering the **tms consumer registration** command on a consumer in privileged EXEC mode. This command is unaffected by registration timer configuration and can be used to register the consumer if the count has been exceeded for implicit registration.

Examples

The following example configures a consumer to send up to five registration messages to a controller:

```
Router(config)# parameter-map type tms PARAMAP_1
Router(config-profile)# controller ipv4 10.1.1.1
Router(config-profile)# logging tms events
Router(config-profile)# registration retry interval 60
Router(config-profile)# registration retry count 5
Router(config-profile)# exit
```

Related Commands

Command	Description
parameter-map type tms	Configures a TMS type parameter map.
registration retry interval	Configures the length of time between consumer registration attempts.

registration retry interval

To configure the length of time between consumer registration attempts, use the **registration retry interval** command in parameter-map configuration mode. To configure the consumer to use the default registration timer interval, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **registration retry interval** command is not available in Cisco IOS software.

registration retry interval *time*

no registration retry interval *time*

Syntax Description

time	Time, in seconds, between registration attempts. A number from 30 through 3000 can be entered for the *seconds* argument.

Command Default

The following default value is used if this command is not configured or if the **no** form is entered:

180

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **registration retry interval** command is entered on a consumer to configure the time interval between the transmission of implicit registration request messages.

The consumer must register with the controller before the controller can send Control Information Messages (CIMs). Implicit registration requests are automatically sent to the controller when a Transitory Messaging Services (TMS) type service policy is activated on the consumer.

By default, a consumer sends a registration request message to the controller once every 3 minutes for up to three times or until successfully registered. If the consumer is a member of multiple groups, it sends a separate registration request messages to the controller of each group.

Note Explicit registration is configured by entering the **tms consumer registration** command on a consumer in privileged EXEC mode. This command is unaffected by registration timer configuration and can be used to register the consumer if the count has been exceeded for implicit registration.

Examples

The following example configures a consumer to send registration messages at 60-second intervals:

```
Router(config)# parameter-map type tms PARAMAP_1
Router(config-profile)# controller ipv4 10.1.1.1

Router(config-profile)# logging tms events
Router(config-profile)# registration retry interval 60

Router(config-profile)# registration retry count 5

Router(config-profile)# exit
```

Related Commands

Command	Description
parameter-map type tms	Configures a TMS type parameter map.
registration retry count	Configures the number of times that a registration message is sent to a controller.

registration retry-interval (TIDP)

To configure the length of time and number of attempts for TIDP group registration, use the **registration retry-interval** command in TIDP group configuration mode. To configure TIDP to use default registration timer values, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **registration retry-interval** command is not available in Cisco IOS software.

registration retry-interval min *interval* **max** *interval*

no registration retry-interval

Syntax Description

min*interval*	Time interval, in seconds, at which TIDP attempts to register a group member. This argument is entered as a number from 0 through 65000.
max*interval*	Total time, in seconds, TIDP attempts to register a TIDP group member. The value for this argument can be a number from 0 through 65000.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

min 60 **max** 3600

Command Modes

TIDP group configuration (config-tidp-grp)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The controller registers consumers. By default, the controller sends a registration request message once every 60 seconds for up to 1 hour until the consumer is successfully registered. The value entered for the **max** keyword must be equal to or greater than the value entered for the **min** keyword. Entering a value of zero after both the **min** and **max** keywords configures the controller not to retry registration if the initial registration message receives no response.

Examples

The following example configures TIDP to attempt to register group members at 30-second intervals for up to 10 minutes or until consumers are registered:

```
Router(config)# tidp group 10

Router(config-tidp-grp)# key-set KEY_1

Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.1

Router(config-tidp-grp)# peer 10.1.1.2

Router(config-tidp-grp)# peer 10.1.1.3

Router(config-tidp-grp)# active
```

Related Commands

Command	Description
active	Activates a TIDP group.
key-set	Configures a key set for a TIDP group.
peer	Configures a consumer as a member of a TIDP group.
tidp group	Configures a TIDP group.

rekey address ipv4

To specify the source or destination information of the rekey message, use the **rekey address ipv4** command in GDOI local server configuration mode. To remove a source or destination address, use the **no** form of this command.

rekey address ipv4 {*access-list-number*| *access-list-name*}

no rekey address ipv4 {*access-list-number*| *access-list-name*}

Syntax Description

access-list-number	IP access list number. The number can be from 100 through 199, or it can be in the expanded range of 2000 through 2699.
access-list-name	Access list name.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

The source is usually the key server interface from which the message leaves, and the destination is the multicast address on which the group members receive the rekeys (for example, access-list 101 permit 121 permit udp host 10.0.5.2 eq 848 host 192.168.1.2. eq 848).

Examples

The following example shows that the rekey address is access list “101”:

```
rekey address ipv4 101
```

The following example shows that a rekey message is to be sent to access control list (ACL) address 239.10.10.10:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
```

access-list 120 permit udp host 10.5.90.1 eq 848 host 239.10.10.10 eq 848

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey algorithm

To define the type of encryption algorithm used for a Group Domain of Interpretation (GDOI) group, use the **rekey algorithm** command in GDOI local server configuration mode. To disable an algorithm that was defined, use the **no** form of this command.

rekey algorithm *type-of-encryption-algorithm*

no rekey algorithm *type-of-encryption-algorithm*

Syntax Description

type-of-encryption-algorithm	Type of encryption algorithm used (see the table below). The default algorithm is 3des-cbc. • The rekey algorithm is used to encrypt the rekey message that is sent from the key server to the multicast group.

Command Default

If this command is not configured, the default value of 3des-cbc takes effect. However, the default is used only if the commands required for a rekey to occur are specified (see the Note below in "Usage Guidelines").

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The table below lists the types of encryption algorithms that may be used.

Table 21: Types of Encryption

Encryption Type	Description
3des-cbc	Cipher Block Chaining mode of the Triple Data Encryption Standard (3des).

Encryption Type	Description
aes 128	128-bit Advanced Encrytion Standard (AES).
aes 192	192-bit AES.
aes 256	256-bit AES.
des-cbc	Cipher Block Chaining mode of the Data Encryption Standard (des).

At a minimum, the following commands are required for a rekey to occur:

rekey address ipv4 {*access-list-number*| *access-list-name*}

rekey authentication {**mypubkey** | **pubkey**} {*rsa key-name*}

If the **rekey algorithm** command is not configured, the default of 3des-cbc is used if the above minimum rekey configuration is met.

Examples

The following example shows that the 3des-cbc encryption standard is used:

```
rekey algorithm 3des-cbc
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
rekey address ipv4	Specifies the source or destination information of the rekey message.
rekey authentication	Specifies the keys to be used to a rekey to GDOI group members.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey authentication

To specify the keys to be used for a rekey to Group Domain of Interpretation (GDOI) group members, use the **rekey authentication**command in GDOI local server configuration mode. To disable the keys, use the **no** form of this command.

rekey authentication {**mypubkey**| **pubkey**} **rsa** *key-name*

no rekey authentication {**mypubkey**| **pubkey**} **rsa** *key-name*

Syntax Description

mypubkey	Keypair associated with this device.
pubkey	Public key associated with a different device.
rsa	Identifies an Rivest, Shamir, and Adelman (RSA) keypair.
key-name	Key to be used for rekey.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(24)T	This command was modified. The **pubkey** keyword was removed.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

For this command to work, Rivest, Shamir, and Adelman (RSA) keys must be generated first on the router using the following command:

crypto key generate rsa {**general keys**} [**label** *key-label*]

For example:

```
crypto key generate rsa general keys label group_1234_key_name
```

Examples

The following example shows that the keypair to be used for a rekey is RSA “group_1234_key_name”:

```
rekey authentication mypubkey rsa group_1234_key_name
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
crypto key generate rsa	Generates RSA key pairs.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey lifetime

To limit the number of days or seconds for which any one key encryption key (KEK) should be used, use the **rekey lifetime** command in GDOI local server configuration mode. To disable the number of days or seconds that were set, use the **no** form of this command.

rekey lifetime {**days** *number-of-days*| **seconds** *number-of-seconds*}

no rekey lifetime {**days**| **seconds**}

Syntax Description

number-of-days	Lifetime in days. The range is 1 to 30.
number-of-seconds	Lifetime in seconds. The range is 300 to 2592000.

Command Default

1 day (86400 seconds).

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.3(2)T	This command was modified. The **days** *number-of-days* keyword and argument pair was added, and the maximum value for the **seconds** *number-of-seconds* keyword and argument pair was extended from 86400 seconds to 2592000 seconds.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

When the rekey lifetime is reached, a new KEK is sent to the group members so that the next rekey is encrypted with the new KEK.

Examples

The following example shows how to set the rekey lifetime to 600 seconds:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey lifetime seconds 600
Device(gdoi-local-server)# end
```

Related Commands

Command	Description
crypto gdoi group	Creates or identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey retransmit

To specify the duration of a rekey message retransmission and the number of retransmissions, use the **rekey retransmit** command in GDOI local server configuration mode. To disable the duration and number that were specified, use the **no** form of this command.

rekey retransmit *number-of-seconds* {**number** *number-of-retransmissions*| **periodic**}

no rekey retransmit

Syntax Description

number-of-seconds	Number of seconds that the rekey message is retransmitted. The range is 10 to 60.
periodic	Periodically sends retransmit rekeys.

Command Default

10 seconds and 2 transmissions.

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.3(2)T	This command was modified. The **periodic** keyword was added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

Use this command if you are concerned about network loss.

The **periodic** keyword sends periodic reminder rekeys to group members (GMs) that did not respond with an acknowledgment in the last scheduled rekey. Combining this keyword with the long SA lifetime feature makes a KS effectively synchronize GMs in case they miss a scheduled rekey before the keys roll over.

Each periodic rekey increments the sequence number, just as for rekey retransmissions. Also, the GM is removed from the GM database on the key server (KS) after three scheduled rekeys (not retransmissions) for which the GM does not send an acknowledgment.

Examples

The following example shows how to specify that the rekey message is retransmitted three times for 15 seconds each time:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 15 number 3
Device(gdoi-local-server)# end
```

Examples

The following example shows how to specify that the rekey message is retransmitted periodically for 30 seconds each time:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GROUP-GDOI
Device(config-gdoi-group)# identity number 4444
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 30 periodic
Device(gdoi-local-server)# end
```

Related Commands

Command	Description
crypto gdoi group	Creates or identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey sig-hash algorithm

To configure the signature hash algorithm for a key encryption key (KEK), use the **rekey sig-hash algorithm** command in GDOI local server configuration mode. To return a signature hash algorithm to the default (SHA-1), use the **no** form of this command.

rekey sig-hash algorithm *algorithm*

no rekey sig-hash algorithm

Syntax Description

algorithm	Signature hash algorithm. You can specify **sha** (for SHA-1), **sha256**, **sha384**, or **sha512**.

Command Default

SHA-1

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Using SHA-1 guarantees interoperability with group members (GMs) that are running earlier versions of Cisco IOS software. Suite B requires SHA-256, SHA-384, or SHA-512.

Examples

The following example shows how to configure the signature hash algorithm to use SHA-512:

```
Device# crypto gdoi group GETVPN
Device(config-gdoi-group) server local
Device(gdoi-local-server) rekey sig-hash algorithm sha512
```

Related Commands

Command	Description
rekey algorithm	Defines the type of encryption algorithm used for a GDOI group.

rekey transport unicast

To configure unicast delivery of rekey messages to group members, use the **rekey transport unicast**command in global configuration mode. To remove unicast delivery of rekey messages and enable the default to multicast rekeying, use the **no** form of this command.

rekey transport unicast

no rekey transport unicast

Syntax Description

This command has no arguments or keywords.

Command Default

If **rekey transport unicast** is not specified or **no rekey transport unicast** is specified, multicast rekeying is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server under the **server local** command, along with other rekey configurations.

Examples

The following example shows that unicast delivery of rekey messages to group members has been configured:

```
crypto gdoi group diffint
 identity number 3333
 server local
  rekey lifetime seconds 300
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa mykeys
  rekey transport unicast
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 64
   address ipv4 10.0.5.2
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the remark command in access list configuration mode. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description

remark	Comment that describes the access-list entry, up to 100 characters long.

Command Default

The access-list entries have no remarks.

Command Modes

Standard named or extended named access list configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples

In the following example, the host1 subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.69.2.88 any eq telnet
```

Related Commands

Command	Description
access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark**command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

remark *text-string*

no remark *text-string*

Syntax Description

text-string	Comment that describes the access list entry, up to 100 characters long.

Command Default

IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **remark** (IPv6) command is similar to the **remark** (IP) command, except that it is IPv6-specific.

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet.

```
ipv6 access-list TELNETTING
 remark Do not allow Marketing subnet to telnet out
 deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

replay counter window-size

To turn on counter-based anti-replay protection for traffic defined inside an access list using Group Domain of Interpretation (GDOI) if there are only two group members in a group, use the **replay counter window-size**command in GDOI SA IPsec configuration mode. To disable counter-based anti-replay protection, use the **no** form of this command.

replay counter window-size [*number*]

no replay counter window-size

Syntax Description

number	Size of the Sychronous Anti-Replay (SAR) clock window expressed in bytes. Values are equal to 64, 128, 256, 512, and 1024 bytes. Default window size is 64 bytes.

Command Default

Counter-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server.

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size in bytes, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

Note GDOI anti-replay can be either counter based or time based. Use this command for counter-based anti-replay protection. For time-based anti-replay protection, use the **replay time window-size** command.

Examples

The following example shows that the anti-replay window size for unicast traffic has been set to 512:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
 sa ipsec 10
   profile group1111
   match address ipv4 101
   replay counter window-size 512
```

Related Commands

Command	Description
replay time window-size	Sets the the window size for anti-replay protection using GDOI if there are more than two group members in a group.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

replay time window-size

To set the window size for anti-replay protection using Group Domain of Interpretation (GDOI) if there are more than two group members in a group, use the **replay time window-size**command in GDOI SA IPsec configuration mode. To disable time-based anti-replay, use the **no** form of this command.

replay time window-size seconds

no replay time window-size

Syntax Description

seconds	Number of seconds of the interval duration of the Sychronous Anti-Replay (SAR) clock. The value range is 1 through 100. The default value is 100.

Command Default

Time-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on the key server.

Note GDOI anti-replay can be either counter based or time based. This command turns on time-based anti-replay. For counter-based anti-replay protection, use the **replay counter window-size** command.

Examples

The following example shows that the number of seconds of the interval duration of the SAR clock has been set to 1:

```
sa ipsec 10
 profile group1111
 match address ipv4 101
 replay time window-size 1
```

Related Commands

Command	Description
replay counter window-size	Sets the window size for counter-based anti-replay protection for unicast traffic defined inside an access list.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

request-method

To permit or deny HTTP traffic according to either the request methods or the extension methods, use the **request-method**command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

request-method {**rfc** *rfc-method*| **extension** *extension-method*} **action** {**reset**| **allow**} **[alarm]**

no request-method {**rfc** *rfc-method*| **extension** *extension-method*} **action** {**reset**| **allow**} **[alarm]**

Syntax Description

rfc	Specifies that the supported methods of RFC 2616, *Hypertext Transfer Protocol--HTTP/1.1* , are to be used for traffic inspection.
rfc-method	Any one of the following RFC 2616 methods can be specified: **connect**, **default, delete**, **get**, **head**, **options**, **post**, **put**, **trace**.
extension	Specifies that the extension methods are to be used for traffic inspection.
extension-method	Any one of the following extension methods can be specified: **copy**, **default, edit**, **getattribute**, **getproperties**, **index**, **lock**, **mkdir**, **move**, **revadd**, **revlabel**, **revlog**, **save**, **setattribute**, **startrev**, **stoprev**, **unedit, unlock**.
action	Methods and extension methods outside of the specified method are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If a given method is not specified, all methods and extension methods are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only methods configured by the **request-method** command are allowed thorough the firewall; all other HTTP traffic is subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

request-queue (GTP)

To specify the number of General Packet Radio Service (GPRS) Tunneling Protocol (GTP) requests that can be queued to wait for a response, use the **request-queue** command in parameter-map type inspect configuration mode. To remove the specified number of GTP requests queued, use the **no** form of this command.

request-queue *max-requests*

no request-queue

Syntax Description

max-requests	Maximum number of GTP requests that are queued to wait for a response. Valid values are from 1 to 4294967295. The default is 200.

Command Default

By default, 200 GTP requests are queued to wait for a response.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

The **request-queue** command specifies the maximum number of GTP requests that can be queued to wait for a response. When the specified maximum limit is reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, Version Not Supported, and Serving GPRS Support Node (SGSN) Context Acknowledge messages are considered as requests and these messages will not be part of the request queue.

Examples

The following example shows how to configure the GTP request queue size as 2345:

```
Device(config)# parameter-map type inspect-global gtp
Device(config-profile)# request-queue 2345
Device(config-profile)#
```

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

request-timeout

To set the number of seconds before an authentication request times out, use the **request-timeout**command in webvpn sso server configuration mode.

request-timeout *number-of-seconds*

no request-timeout *number-of-seconds*

Syntax Description

number-of-seconds	Number of seconds. Value = 10 through 30. Default = 15.

Command Default

None

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

Examples

The following example shows that the number of seconds before an authentication request times out is 25:

```
webvpn context context1
 sso-server test-sso-server
  request-timeout 25
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

reset (policy-map)

To reset an SMTP connection with an SMTP sender (client) if it violates the specified policy, use the **reset** command in policy-map configuration mode. This action sends an error code to the sender and closes the connection gracefully.

reset

Command Default No default behavior or values.

Command Modes Policy-map configuration

Command History

12.4(20)T	This command was introduced in Cisco IOS Release 12.4(20)T.

Examples The following example displays the reset command configuration for DSP 1:

```
Router(config)# policy-map type inspect smtp p1
Router(config-pmap)# class type inspect smtp c1
Router(config-pmap)# reset
```

reset (zone-based policy)

To reset a TCP connection if the data length of the Simple Mail Transfer Protocol (SMTP) body exceeds the value that you configured in the **class-map type inspect smtp**command, use the **reset** command in policy-map configuration mode.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

The TCP connection is not reset.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

You can enter **reset** only for TCP traffic.

Examples

The following example creates a Layer 7 SMTP policy map named mysmtp-policy and applies the reset action to each of the match criteria:

```
policy-map type inspect smtp mysmtp-policy
 class-map type inspect smtp huge-mails
  reset
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

responder-only

To configure a device as responder-only, use the **responder-only**command in IPsec profile configuration mode. To remove the responder-only setting, use the no form of this command.

responder-only

no responder-only

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not configured as responder-only.

Command Modes

IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

This command is relevant only for a virtual interface scenario and is configurable only under an IPsec profile. Neither static nor crypto maps are supported.

Examples

The following example shows that the device has been configured as a responder-only:

```
crypto ipsec profile vti
 set transform-set 3dessha
 set isakmp-profile clients
 responder-only
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.

retired (IPS)

specify whether or not a retired signature or signature category definition should be saved in the router memory, use the **retired**command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

retired {**true**| **false**}

no retired

Syntax Description

true	Retires all signatures within a given category.
false	“Unretires” all signatures within a given category.

Command Default

Signature or signature category definitions are not saved in the system.

Command Modes

Signature-definition-status configuration (config-sigdef-status) IPS-category-action configuration (config-ips-category-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a “top-down” order, you should first retire all signatures, followed by “unretiring” specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

Examples

The following example shows how to retire all signatures and configure the Basic “ios_ips” category:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
```

```
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
enabled	Changes the enabled status of a given signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Enters the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature.

retransmit (config-radius-server)

To specify the number of times a RADIUS request is re-sent to a server when that server is not responding or responding slowly, use the **retransmit** command in RADIUS server configuration mode. To restore the default value, use the **no** form of this command.

retransmit *retries*

no retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The range is from 0 to 100. The default is 3.

Command Default

The default number of retransmission attempts is 3.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the router, it is recommended that you configure the RADIUS server retransmit rate to 5.

Examples

The following example shows how to specify a retransmit counter value of five times:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# retransmit 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

Command	Description
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

Effective with Cisco IOS Release 12.4(15)T

reverse-route [**static**| **remote-peer** *ip-address* **[gateway] [static]**]

no reverse-route [**static**| **remote-peer** *ip-address* **[gateway] [static]**]

Before Cisco IOS Release 12.4(15)T

reverse-route [**static**| **tag** *tag-id* **[static]**| **remote-peer [static]**| **remote-peer** *ip-address* **[static]**]

no reverse-route [**static**| **tag** *tag-id* **[static]**| **remote-peer [static]**| **remote-peer** *ip-address* **[static]**]

Syntax Description

tag *tag-id*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. **Note** Effective with Cisco IOS Release 12.4(15)T, the **tag** keyword and *tag-id* argument were removed.
remote-peer	(Optional) Indicates two routes: one for the tunnel endpoint, with the next hop being the interface to which the crypto map is bound. **Note** The **remote-peer** keyword and its variants (*ip-address* argument and **gateway** keyword) are applicable only to crypto maps.
ip-address	(Optional) If this argument is used without the optional **gateway** keyword, there is only one route: the protected subnet. The next hop is determined by the user-added value for the *ip-address* argument.
gateway	(Optional) Used with the *ip-address* argument. If the **gateway** keyword is used, there are two routes: one to the protected subnet through the remote-tunnel endpoint and the other to the remote-tunnel endpoint that is determined by the user-added value for the *ip-address* argument. **Note** The optional **gateway** keyword enables the behavior of the **reverse-route remote-peer** *ip-address* command syntax used for software releases before Cisco IOS Release 12.3(14)T.

static	(Optional) Creates routes on the basis of crypto ACLs, regardless of whether flows have been created for these ACLs.

Command Default

No default behavior or values.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The **remote-peer** keyword and *ip-address* argument were added.
12.3(14)T	The **static** and **tag** keywords and *tag-id* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The **tag** keyword and *tag-id* argument were deleted. The **gateway** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelin

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

This command can be applied on a per-crypto map basis.

Reverse route injection (RRI) provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.

When enabled in an IPSec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPsec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

The **remote-peer** keyword is required when RRI is performed in a VRF-Aware IPsec scenario.

Examples

Examples

The following example shows how to configure RRI when crypto ACLs exist. The example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto ACL.

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102
Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Note In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword will be necessary, that is, **reverse-route static.**

The **reverse-route** command in this situation creates routes that are analogous to the following static route CLI (**ip route**):

- Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

- VPN Services Module (VPNSM)

```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured.

```
reverse-route remote-peer
```

Examples

The following configuration example shows how to configure RRI for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
```

```
   match address 101
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5
router ospf 109
 redistribute rip route-map rip-to-ospf
route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Device# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

The following example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The previous example yields the following before Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
 table)
```

Examples

In the following example, routes are created from the destination information in the access control list (ACL). One route will list 10.2.2.2 as the next-hop route to the ACL information, and one will indicate that to get to 10.2.2.2, the route will have to go via 10.1.1.1. All routes will have a metric of 10. Routes are created only at the time the map and specific ACL rule are created.

```
crypto map map1 1 ipsec-isakmp
 set peer 10.2.2.2
 reverse-route remote-peer 10.1.1.1 gateway
 set reverse-route distance 10
 match address 101
Configuring RRI with Route Tags 12.4(15)T or later: Example
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5
router ospf 109
 redistribute rip route-map rip-to-ospf
route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Device# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
show crypto map (IPSec)	Displays the crypto map configuration.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

revocation-check *method1* [*method2 method3*]

no revocation-check *method1* [*method2 method3*]

Syntax Description

method1 [*method2 method3*]	Method used by the device to check the revocation status of the certificate. Available methods are as follows: • **crl—**Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none—**Certificate checking is not required. • **ocsp—**Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

Command Default

After a trustpoint is enabled, the default is set to **revocation-check crl**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the **crl best-effort** and **crl optional** commands.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the**revocation-check** command to specify at least one method that is to be used to ensure that the certificate of a peer has not been revoked.

If your device does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your device will reject the peer's certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

Your device will process a CRL in the Distinguished Encoding Rules (DER) format only. Revocation check will fail and will be rejected if the CRL is in any other format, such as, Privacy Enhanced Mail (PEM) format.

Note The **none** keyword replaces the **optional** keyword that is available from the **crl** command. If you enter the **crl optional** command, it will be written back as the **revocation-check none** command. However, there is a difference between the **crl optional** command and the **revocation-check none**command. The **crl optional** command will perform revocation checks against any applicable in-memory CRL. If a CRL is not available, a CRL will not be downloaded and the certificate is treated as valid; the **revocation-check none** command ignores the revocation check completely and always treats the certificate as valid. Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the device to use the OCSP server that is specified in the AIA extension of the certificate:

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# revocation-check ocsp
```

The following example shows how to configure the device to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# revocation-check crl ocsp
```

The following example shows how to configure your device to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# ocsp url http://myocspserver:81
Device(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your device should use.
ocsp url	Enables an OCSP server.

revocation-check (ca-trustpool)

To disable a revocation checking method when the public key infrastructure (PKI) trustpool policy is being used, use the **revocation-check** command in ca-trustpool configuration mode. To return to the default, use the **no** form of this command.

revocation-check *method1* [*method2 method3*]

no revocation-check *method1* [*method2 method3*]

Syntax Description

method1 [*method2 method3*]]	Method used by the router to check the revocation status of the certificate. Available methods are identified by the following keywords: • **crl**--Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none** --Certificate checking is not required. • **ocsp**--Certificate checking is performed by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down.

Command Default

CRL checking is mandatory for current trustpoint policy usage.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

If a revocation policy needs to be altered for specific certificate authority (CA) certificates in the PKI trustpool, use certificate maps instead.

Your device will process a CRL in the Distinguished Encoding Rules (DER) format only. Revocation check will fail and will be rejected if the CRL is in any other format, such as, Privacy Enhanced Mail (PEM) format.

Examples

The **revocation-check** command in following example disables both CRL and OCSP revocation checks:

```
Device(config)# crypto pki trustpool policy
Device(ca-trustpool)# revocation-check ocsp crl none
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration subcommand to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.

Command	Description
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

root tftp *server-hostname filename*

no root tftp *server-hostname filename*

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
server-hostname filename	Specifies a name for the server and a name for the file that will store the trustpoint CA.

Command Default

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint**command , which puts you in ca-trustpoint configuration mode.

Note The **crypto ca trustpoint**commanddeprecates the **crypto ca identity**and **crypto ca trusted-root**commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, theconfiguration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
 root tftp xxx fff
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

root CEP

The **crypto ca trustpoint**commanddeprecates the **crypto ca trusted-root**command and all related subcommands (all trusted-root configuration mode commands). If you enter a trusted-root subcommand, theconfiguration mode and command will be written back as ca-trustpoint.

root PROXY

The **root PROXY**command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy**command for more information.

root TFTP

The **root TFTP**command is replaced by the **root** command. See the **root**command for more information.

route accept

To filter the routes received from the peer and save the routes on the router based on the specified values, use the **route accept** command in IKEv2 authorization policy configuration mode. To reject the routes , use the **no** form of this command.

route accept any [**tag** *tag-id*] [**distance** *value*]

no route accept

Syntax Description

any	Accepts all routes received from the peer.
tag *tag-id*	(Optional) Tags the route with the specified ID. The default value is 1.
distance *value*	(Optional) Sets the metric of the route with the specified value. The default value is 2.

Command Default

The routes received from the peer are not filtered.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Before using the **route accept** command, you must first configure the **crypto ikev2 authorization policy** command.

Examples

The following example show how to filter the routes received from the peer and save the routes on the router based on the specified values:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# route accept any tag 1
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

route set

To specify the route set parameters to the peer via configuration mode, use the **route set** command in IKEv2 authorization policy configuration mode. To disable, use the **no** form of this command.

route set {**interface** *interface*| **access-list** {*access-list-name*| *access-list-number*| *expanded-access-list-number*| **ipv6** *access-list-name*}}

no route set {**interface**| **access-list** {*access-list-name*| *access-list-number*| *expanded-access-list-number*| **ipv6** *access-list-name*}}

Syntax Description

interface *interface*	Specifies the route interface.
access-list	Specifies the route access list.
access-list-name	Specifies the access list name.
access-list-number	Specifies the standard access list number. The range is from 1 to 99.
expanded-access-list-number	Specifies the expanded access list number. The range is from 1300 to 1999.
ipv6	Specifies an IPv6 access list.

Command Default

Route set parameters are not set.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.2(2)T	This command replaces the **subnet-acl** command.
15.3(3)M	This command was modified. The *interface* argument was added.

Usage Guidelines

Before using the **route set** command, you must first configure the **crypto ikev2 authorization policy** command. This command allows running routing protocols such as BGP over VPN.

Examples

The following example show how to send the IP address of the VPN interface to the peer via configuration mode:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# route set interface Ethernet
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

route set remote

To push route set parameters to be pushed to the remote peer via configuration mode, use the **route set remote** command in IKEv2 authorization policy configuration mode. To disable, use the **no** form of this command.

route set remote{**ipv4***ip-address mask*| **ipv6***ip-address*/*mask*}

no route set remote{**ipv4***ip-address mask*| **ipv6***ip-address*/*mask*}

Syntax Description

ipv4	Specifies an IPv4 route.
ipv6	Specifies an IPv6 route.
ip-address mask	The IP address and network mask for the route.

Command Default

Route set parameters are not set.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Before using the **route set remote** command, you must first configure the **crypto ikev2 authorization policy** command.

Examples

The following example show how to push an IPv4 address to the remote peer via configuration mode:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# route set ipv4 10.0.0.1 255.255.255.0
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in RA guard policy configuration mode.

router-preference maximum {**high**| **low**| **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default routers advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised default router preference is set to **high** in the received packet, then the packet is dropped. If the command option is set to **medium** or **low** in the received packet, then the packet is not dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures router-preference maximum verification to be high:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# router-preference maximum high
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

rsakeypair

To specify which Rivest, Shamir, and Adelman (RSA) key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

rsakeypair *key-label* [*key-size* [*encryption-key-size*]]

Syntax Description

key-label	Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
key-size	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key pair. If the size is not specified, the existing key size is used.
encryption-key-size	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Command Default

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was added.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair “exampleCAkeys”:

```
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during Internet Key Exchange (IKE) authentication, use the **rsa-pubkey**command in keyring configuration mode. To remove the manual key that was defined, use the **no** form of this command.

rsa-pubkey {**address** *address*| **name** *fqdn*} [**encryption**| **signature**]

no rsa-pubkey {**address** *address*| **name** *fqdn*} [**encryption**| **signature**]

Syntax Description

address *address*	IP address of the remote peer.
name *fqdn*	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Command Default

No default behavior or values

Command Modes

Keyring configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
```

```
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```