Machete Router

NIAP Configuration Parameters

VERSION 1.1

DECEMBER 8, 2023

Version History:

Version	Date	Change Description
1.0	11/22/2023	Initial draft.
1.1	12/08/2023	Updated to reflect current version

Table of Contents

Table of Figures

1 Introduction

The Machete router is a ruggedized, compact, secure and high-performance router that also provides VPN gateway and WLAN Access System functionality. The routing functions of Machete are implemented in a software suite titled the ATCorp Routing and Encryption Suite (ARES).

This document provides a list of configuration parameters available to the Machete Router when operating in the Common Criteria-approved mode of operation in accordance with collaborative Protection Profile for Network Devices version 2.0 (NDcPP) and NDcPP/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway version 2.1 (VPNGWcEP).

1.1 Reference Documents

Document ID	Document Name	Version	Date
Machete CCOG	Architecture Technology Corporation Machete Router Common Criteria Operational Guidance	1.4	12/08/2023

Figure 1: Reference Documents

1.2 Audience

This document is intended for administrators configuring the Machete router. This document assumes the user is familiar with networks and network terminology and is a trusted individual.

2 ARES Configuration Parameters

This section details the complete collection of the NIAP compliant configuration parameters available for the ARES service.

2.1 Top-Level ARES JSON

Description: The outer-most JSON object {} that encases all other parameters.
Type: JSON Object

2.2 SecurityMode

Property: SecurityMode
Description: The security mode ARES should adhere to when validating the configuration
Type: Enum of normal, niap, csfc.

Default: normal

2.3 Log

Property: Log
Description: The logging configuration.
Type: JSON Object
Default: None

2.3.1 Dest

Property: Log :: Dest
Description: Log destinations. "StdOut" and "Syslog" are special destinations, all others are interpreted as a file name.
Type: Array with a minimum number of 1 item(s) that must be unique.
Default: /var/log/ares/ares.log
Type: Refer to - definitions->types->File_Dir
Default: None

2.3.2 Buckets

Property: Log :: Buckets
Description: Array of log bucket names enabled for logging. Some buckets have sub-bucket options, if the top level bucket is enabled, that enables all the sub-buckets as well. Default is all enabled.
Type: Array of unique items.
Type: Refer to - definitions->logging->LogBuckets
Default: None

Verbosity

2.3.3 Property: Log :: Verbosity

Description: Value indicating the level of verbosity when writing log messages.
Default: error
Type: Refer to - definitions->logging->LogVerbosity
Default: None

2.3.4 KernelVerbosity

Property: Log :: KernelVerbosity
Description: Value indicating the level of verbosity when writing kernel log messages. Higher verbosity means more logging.
Default: error
Type: Refer to - definitions->logging->LogVerbosity
Default: None

2.3.5 Audit

Property: Log :: Audit

Description: Audit server options.
Type: JSON Object
Default: None

2.3.5.1 Syslog
Property: Log :: Audit :: Syslog
Description: Remote syslog server configuration.
Type: JSON Object
Required: ['IPAddress']
Default: None

2.3.5.1.1 IPAddress
Property: Log :: Audit :: Syslog :: IPAddress
Description: IPv4 address of the remote syslog server.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.3.5.1.2 Port
Property: Log :: Audit :: Syslog :: Port
Description: Port used to communicate with the remote syslog server.
Type: Refer to - definitions->types->UINT16
Default: 514

2.3.5.1.3 Protocol
Property: Log :: Audit :: Syslog :: Protocol
Description: Protocol used to communicate with the remote syslog server.
Type: String enum of tcp, udp.
Default: tcp

2.4 RouterName

Property: RouterName
Description: The descriptive name of this router. Defaults to the hostname. If set, it changes the hostname.
Type: Refer to - definitions->types->AlphaNumeric
Default: None

2.5 RouterId

Property: RouterId
Description: A unique identifier for each router in the network.
Type: Refer to - definitions->types->UINT32
Or
Type: Refer to - definitions->types->DottedQuad

Default: None

2.6 ConfigVersion

Property: ConfigVersion
Description: A user defined version string for this configuration.
Type: String.
Default: None

2.7 ConfigDescription

Property: ConfigDescription
Description: A user defined description for this configuration.
Type: String.
Default: None

2.8 Links

Property: Links
Description: An array of link objects.
Type: Array of unique items.
Item description: Describes the configuration of the link.
Item type: JSON Object
Required: ['Name', 'Type', 'Interface']
Default: None

2.8.1 Name

Property: Links :: Name
Item description: A descriptive name of this link.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.2 Type

Property: Links :: Type
Item description: The type of the ARES link.
Item type: String enum of simple, host, boundary, wan, core, edge.
Default: None

2.8.3 Interface

Property: Links :: Interface
Item description: Options that define the interface for this link.
Item type: JSON Object
Default: None

2.8.3.1 Type

Property: Links :: Interface :: Type
Item description: The type of interface.
Item type: String enum of physical, tunnel, vrf, vlan, vxlan, pppoe, dummy, bond, veth, bridge, tuntap, wifi.
Default: physical

2.8.3.2 HardwareAddress

Property: Links :: Interface :: HardwareAddress
Item description: The hardware address of the device. This is the primary device identifier used when set. Only applicable for physical interfaces.
Type: Refer to - definitions->types->HardwareAddress
Default: None

2.8.3.3 Name

Property: Links :: Interface :: Name
Item description: The name of the interface. This is the device identifier used if Hardware Address is not set. For physical interfaces, if Hardware Address is used, then the interface name will be changed to match the one given; otherwise name is required and ARES will create the device with this name.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.4 Inet4Addresses

Property: Links :: Interface :: Inet4Addresses
Item description: The IPv4 addresses for the interface. The first address is used as the primary address, and for physical interfaces, this is the last device identifier used if neither Hardware Address nor Name are set. Required for virtual and tunnel interfaces. Setting "auto" will perform DHCP to get the IPv4 address.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4MaskReq
Or
Item type: String enum of auto.
Default: None

2.8.3.5 Inet6Addresses

Property: Links :: Interface :: Inet6Addresses
Item description: The IPv6 addresses for the interface. Setting "auto" will perform DHCP to get the IPv4 address.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv6MaskReq
Or
Item type: String enum of auto.

Default: None

2.8.3.6 KeepDHCP4Gateway

Property: Links :: Interface :: KeepDHCP4Gateway
Item description: If set to true, keep the default gateway route added by DHCP for IPv4. Default is to ignore the default route.
Item type: Boolean true or false.
Default: False

2.8.3.7 KeepDHCP6Gateway

Property: Links :: Interface :: KeepDHCP6Gateway
Item description: If set to true, keep the default gateway route added by DHCP for IPv6. Default is to ignore the default route.
Item type: Boolean true or false.
Default: False

2.8.3.8 MTU

Property: Links :: Interface :: MTU
Item description: The Maximum Transmission Unit size (bytes).
Item type: Integer with a minimum of 68 and a maximum of 1500.
Default: 1500

2.8.3.9 Flags

Property: Links :: Interface :: Flags
Item description: Flags to customize the operation of this interface.
Item type: JSON Object
Default: None

2.8.3.9.1 Multicast

Property: Links :: Interface :: Flags :: Multicast
Item description: Enable/disable multicast packets on this interface.
Item type: Boolean true or false.
Default: True

2.8.3.9.2 ARP

Property: Links :: Interface :: Flags :: ARP
Item description: Enable/disable ARP on this interface.
Item type: Boolean true or false.
Default: True

2.8.3.9.3 Promiscuous

Property: Links :: Interface :: Flags :: Promiscuous
Item description: Enable/disable Promiscuous mode on this interface.

Item type: Boolean true or false.
Default: False

2.8.3.10 Tunnel

Property: Links :: Interface :: Tunnel
Item description: Configure a tunnel interface.
Item type: JSON Object
Required: ['Local', 'Remote']
Default: None

2.8.3.10.1 Local

Property: Links :: Interface :: Tunnel :: Local
Item description: The address of the local endpoint of the tunnel.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.3.10.2 Remote

Property: Links :: Interface :: Tunnel :: Remote
Item description: The address of the remote endpoint of the tunnel.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.3.10.3 TTL

Property: Links :: Interface :: Tunnel :: TTL
Item description: The TTL of the tunnel. Default inherit from parent.
Type: Refer to - definitions->types->TTL
Default: None

2.8.3.10.4 Key

Property: Links :: Interface :: Tunnel :: Key
Item description: The key of the tunnel where applicable. Default: no key.
Type: Refer to - definitions->types->UINT32
Or
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.3.10.5 Encap

Property: Links :: Interface :: Tunnel :: Encap
Item description: UDP Encapsulation settings.
Item type: JSON Object
Required: ['Type']
Default: None

2.8.3.10.5.1 Type

Property: Links :: Interface :: Tunnel :: Encap :: Type
Item description: Foo-over-UDP (FOU) or Generic-UDP-Encapsulation (GUE).
Type: Refer to - definitions->tunnel->EncapType
Default: None

2.8.3.10.5.2Port
Property: Links :: Interface :: Tunnel :: Encap :: Port
Item description: The local and remote port used for UDP encapsulation. If this is set, it overrides local/remote settings.
Type: Refer to - definitions->types->Port
Default: 44444

2.8.3.10.5.3LocalPort
Property: Links :: Interface :: Tunnel :: Encap :: LocalPort
Item description: The local port used for UDP encapsulation. I.E. The UDP source port. FOU receive maps this port to the GRE protocol.
Type: Refer to - definitions->types->Port
Default: 44444

2.8.3.10.5.4RemotePort
Property: Links :: Interface :: Tunnel :: Encap :: RemotePort
Item description: The remote port used for UDP encapsulation. I.E. The UDP destination port. The other end of the tunnel should map this port to the GRE protocol.
Type: Refer to - definitions->types->Port
Default: 44444

2.8.3.10.6 Keepalive
Property: Links :: Interface :: Tunnel :: Keepalive
Item description: The configuration for the GRE keepalive packets, used only if the GRE keepalive plugin is loaded.
Item type: JSON Object
Required: ['Interval', 'Retries']
Default: None

2.8.3.10.6.1Interval
Property: Links :: Interface :: Tunnel :: Keepalive :: Interval
Item description: The number of seconds between sending keepalive requests.
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.8.3.10.6.2Retries
Property: Links :: Interface :: Tunnel :: Keepalive :: Retries
Item description: The number of failed keepalive requests before bringing down a tunnel.
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.8.3.11 VRF
Property: Links :: Interface :: VRF
Item description: Configuration of a VRF interface.
Item type: JSON Object
Required: ['Table']
Default: None

2.8.3.11.1 Table
Property: Links :: Interface :: VRF :: Table
Item description: The routing table associated with this VRF. Static routes added on this link will automatically be added to this routing table.
Type: Refer to - definitions->types->UINT32
Default: None

2.8.3.11.2 Members
Property: Links :: Interface :: VRF :: Members
Item description: The list of interfaces (or link name) added to this VRF, these interfaces must already exist.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.12 VLAN
Property: Links :: Interface :: VLAN
Item description: Configuration of a VLAN interface.
Item type: JSON Object
Required: ['Parent', 'ID']
Default: None

2.8.3.12.1 Parent
Property: Links :: Interface :: VLAN :: Parent
Item description: The interface name of the parent interface.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.12.2 ID
Property: Links :: Interface :: VLAN :: ID
Item description: The VLAN ID for this interface.
Type: Refer to - definitions->types->VLANIDRange
Default: None

2.8.3.12.3 VXLAN
Property: Links :: Interface :: VXLAN
Item description: Configuration of a VXLAN interface.

Item type: JSON Object
Required: ['ID']
Default: None

2.8.3.12.4 ID
Property: Links :: Interface :: VXLAN :: ID
Item description: Specifies the VXLAN Network Identifer (or VXLAN Segment Identifier) to use.
Type: Refer to - definitions->types->VXLANIDRange
Default: None

2.8.3.12.5 PhysDev
Property: Links :: Interface :: VXLAN :: PhysDev
Item description: Specifies the physical device to use for tunnel endpoint communication.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.12.6 Group
Property: Links :: Interface :: VXLAN :: Group
Item description: Specifies the multicast IP address to join. This parameter cannot be specified with the remote parameter.
Type: Refer to - definitions->types->IPv4Multicast
Default: None

2.8.3.12.7 Remote
Property: Links :: Interface :: VXLAN :: Remote
Item description: Specifies the unicast destination IP address to use in outgoing packets when the destination link layer address is not known in the VXLAN device forwarding database. This parameter cannot be specified with the group parameter.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.3.12.8 Local
Property: Links :: Interface :: VXLAN :: Local
Item description: Specifies the source IP address to use in outgoing packets.
Type: Refer to - definitions->types->IPv4Address
Or
Item type: String enum of any.
Default: None

2.8.3.12.9 TTL
Property: Links :: Interface :: VXLAN :: TTL
Item description: Specifies the TTL value to use in outgoing packets.
Type: Refer to - definitions->types->TTL

Or
Item type: String enum of auto, inherit.
Default: None

2.8.3.12.10 TOS

Property: Links :: Interface :: VXLAN :: TOS
Item description: Specifies the TOS value to use in outgoing packets.
Type: Refer to - definitions->types->UINT8
Or
Item type: String enum of inherit.
Default: None

2.8.3.12.11 DF

Property: Links :: Interface :: VXLAN :: DF
Item description: Specifies the usage of the Don't Fragment flag (DF) bit in outgoing packets with IPv4 headers. The value 'Inherit' causes the bit to be copied from the original IP header. The values unset and set cause the bit to be always unset or always set, respectively. By default, the bit is not set.
Item type: String enum of inherit, set, unset.
Default: None

2.8.3.12.12 Flowlabel

Property: Links :: Interface :: VXLAN :: Flowlabel
Item description: Specifies the flow label to use in outgoing packets.
Item type: Integer with a minimum of 0 and a maximum of 1048575.
Default: None

2.8.3.12.13 DstPort

Property: Links :: Interface :: VXLAN :: DstPort
Item description: Specifies the UDP destination port to communicate to the remote VXLAN tunnel endpoint.
Type: Refer to - definitions->types->Port
Default: None

2.8.3.12.14 SrcPort

Property: Links :: Interface :: VXLAN :: SrcPort
Item description: Specifies the range of port numbers to use as UDP source ports to communicate to the remote VXLAN tunnel endpoint.
Item type: Array of unique items and a minimum number of 2 item(s) and a maximum number of 2 item(s).
Type: Refer to - definitions->types->Port
Default: None

2.8.3.12.15 Learning

Property: Links :: Interface :: VXLAN :: Learning
Item description: Specifies if unknown source link layer addresses and IP addresses are entered into the VXLAN device forwarding database.
Item type: Boolean true or false.
Default: None

2.8.3.12.16 RSC

Property: Links :: Interface :: VXLAN :: RSC
Item description: Specifies if route short circuit is turned on.
Item type: Boolean true or false.
Default: None

2.8.3.12.17 Proxy

Property: Links :: Interface :: VXLAN :: Proxy
Item description: Specifies if ARP proxy is turned on.
Item type: Boolean true or false.
Default: None

2.8.3.12.18 L2Miss

Property: Links :: Interface :: VXLAN :: L2Miss
Item description: Specifies if netlink LLADDR miss notifications are generated.
Item type: Boolean true or false.
Default: None

2.8.3.12.19 L3Miss

Property: Links :: Interface :: VXLAN :: L3Miss
Item description: Specifies if netlink IP ADDR miss notifications are generated.
Item type: Boolean true or false.
Default: None

2.8.3.12.20 UDPCSum

Property: Links :: Interface :: VXLAN :: UDPCSum
Item description: Specifies if UDP checksum is calculated for transmitted packets over IPv4.
Item type: Boolean true or false.
Default: None

2.8.3.12.21 UDP6ZeroCSumTX

Property: Links :: Interface :: VXLAN :: UDP6ZeroCSumTX
Item description: Skip UDP checksum calculation for transmitted packets over IPv6.
Item type: Boolean true or false.
Default: None

2.8.3.12.22 UDP6ZeroCSumRX

Property: Links :: Interface :: VXLAN :: UDP6ZeroCSumRX
Item description: Allow incoming UDP packets over IPv6 with zero checksum field.
Item type: Boolean true or false.
Default: None

2.8.3.12.23 Ageing

Property: Links :: Interface :: VXLAN :: Ageing
Item description: Specifies the lifetime in seconds of FDB entries learnt by the kernel.
Type: Refer to - definitions->types->UINT16
Default: None

2.8.3.12.24 MaxAddress

Property: Links :: Interface :: VXLAN :: MaxAddress
Item description: Specifies the maximum number of FDB entries.
Type: Refer to - definitions->types->UINT16
Default: None

2.8.3.12.25 External

Property: Links :: Interface :: VXLAN :: External
Item description: Specifies whether an external control plane (e.g. ip route encap) or the internal FDB should be used.
Item type: Boolean true or false.
Default: None

2.8.3.12.26 GBP

Property: Links :: Interface :: VXLAN :: GBP
Item description: Enables the Group Policy extension (VXLAN-GBP).
Allows to transport group policy context across VXLAN network peers. If enabled, includes the mark of a packet in the VXLAN header for outgoing packets and fills the packet mark based on the information found in the VXLAN header for incoming packets.
Item type: Boolean true or false.
Default: None

2.8.3.12.27 GPE

Property: Links :: Interface :: VXLAN :: GPE
Item description: Enables the Generic Protocol extension (VXLAN-GPE). Currently, this is only supported together with the external keyword.
Item type: Boolean true or false.
Default: None

2.8.3.12.28 Neighbors

Property: Links :: Interface :: VXLAN :: Neighbors
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: JSON Object

Required: ['IP', 'LLAddrs']
Default: None

2.8.3.12.29 IP
Property: Links :: Interface :: VXLAN :: Neighbors :: IP
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.3.12.29.1 LLAddrs
Property: Links :: Interface :: VXLAN :: Neighbors :: LLAddrs
Type: Refer to - definitions->types->HardwareAddressArr
Default: None

2.8.3.13 PPPoE
Property: Links :: Interface :: PPPoE
Item description: Configuration of a PPPoE interface.
Item type: JSON Object
Required: ['Device', 'Username', 'Password']
Default: None

2.8.3.13.1 Device
Property: Links :: Interface :: PPPoE :: Device
Item description: The name of the device in which PPPoE will be performed.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.13.2 Username
Property: Links :: Interface :: PPPoE :: Username
Item description: The username to authenticate the PPP connection.
Item type: String with a minimum length of 1 and a maximum Length of 32 characters.
Default: None

2.8.3.13.3 Password
Property: Links :: Interface :: PPPoE :: Password
Item description: The password to authenticate the PPP connection. If ends in ".pass" it assumes the password is read from a file with this name.
Item type: String with a minimum length of 8 and a maximum Length of 63 characters.
Default: None

2.8.3.13.4 auth
Property: Links :: Interface :: PPPoE :: auth
Item description: If true, set the "auth" setting, otherwise set the "noauth" setting.
Item type: Boolean true or false.
Default: False

2.8.3.13.5 noipdefault
Property: Links :: Interface :: PPPoE :: noipdefault
Item description: If true, set the "noipdefault" setting which disables the default behaviour when no local IP address is specified, which is to determine (if possible) the local IP address from the hostname. With this option, the peer will have to supply the local IP address during IPCP negotiation.
Item type: Boolean true or false.
Default: True

2.8.3.13.6 defaultroute
Property: Links :: Interface :: PPPoE :: defaultroute
Item description: If true, set the "defaultroute" setting which adds a default route to the system routing tables, using the peer as the gateway, when IPCP negotiation is successfully completed. This entry is removed when the PPP connection is broken.
Item type: Boolean true or false.
Default: False

2.8.3.13.7 replacedefaultroute
Property: Links :: Interface :: PPPoE :: replacedefaultroute
Item description: If true, set the "replacedefaultroute" setting which is a flag to the defaultroute option. If defaultroute is set and this flag is also set, pppd replaces an existing default route with the new default route.
Item type: Boolean true or false.
Default: False

2.8.3.13.8 persist
Property: Links :: Interface :: PPPoE :: persist
Item description: If true, set the "persist" setting, otherwise set the "nopersist" setting. Persistent connections will try to reopen the connection if it is terminated.
Item type: Boolean true or false.
Default: True

2.8.3.14 Bonding
Property: Links :: Interface :: Bonding
Item description: Describes a bound logical interface.
Item type: JSON Object
Default: None

2.8.3.14.1 Interfaces
Property: Links :: Interface :: Bonding :: Interfaces
Item description: An array of interfaces to bond into a single logical interface.
Item type: Array of unique items.
Type: Refer to - definitions->types->InterfaceName

Default: None

2.8.3.14.2 ActiveMember
Property: Links :: Interface :: Bonding :: ActiveMember
Item description: Specifies the ARP new active members for modes that support it.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.14.3 ADActorSysPrio
Property: Links :: Interface :: Bonding :: ADActorSysPrio
Item description: Specifies the 802.3ad system priority.
Item type: Integer with a minimum of 1 and a maximum of 65535.
Default: 65535

2.8.3.14.4 ADActorSystem
Property: Links :: Interface :: Bonding :: ADActorSystem
Item description: Specifies the 802.3ad mac-address for the actor in protocol packet exchange.
Type: Refer to - definitions->types->HardwareAddress
Default: None

2.8.3.14.5 ADSelect
Property: Links :: Interface :: Bonding :: ADSelect
Item description: Specifies the 802.3ad aggregation logic:
Stable - Active aggregator is chosen by largest aggregate bandwidth. Reselection occurs when all members of the active aggregator are down.
Bandwidth - The active aggregator is chosen by the largest aggregate bandwidth. Reselection occurs if any members link state or 802.3ad association state changes.
Count - The active aggregator is chosen by the largest number of ports.
Type: Refer to - definitions->bonding->ADSelect
Default: stable

2.8.3.14.6 ADUserPortKey
Property: Links :: Interface :: Bonding :: ADUserPortKey
Item description: Specifies the 802.3ad port key.
Item type: Integer with a minimum of 1 and a maximum of 65535.
Default: 65535

2.8.3.14.7 AllMembersActive
Property: Links :: Interface :: Bonding :: AllMembersActive
Item description: Specifies that duplicate frames should be dropped (false) or delivered (true).
Item type: Boolean true or false.
Default: false

2.8.3.14.8 ARPInterval

Property: Links :: Interface :: Bonding :: ARPInterval
Item description: Specifies the ARP link monitoring frequency in milliseconds. Should not be used with MIIMon. A value of 0 disables ARP monitoring.
Item type: Integer with a minimum of 0.
Default: 0

2.8.3.14.9 ARPIPTarget

Property: Links :: Interface :: Bonding :: ARPIPTarget
Item description: An array of IP addresses to use as ARP monitoring peers when ARPInterval is > 0. Maximum number of targets is 16.
Item type: Array with a minimum number of 1 item(s) and a maximum number of 16 item(s) that must be unique.
Type: Refer to - definitions->types->IPAddress
Default: None

2.8.3.14.10 ARPValidate

Property: Links :: Interface :: Bonding :: ARPValidate
Item description: Specifies whether ARP probes and replies should be validated in modes that support ARP monitoring.:
None - No validation.
Active - Validation is performed only for the active member.
Backup - Validation is performed only for the backup member.
All - Validation is performed for all members.
Filter - Filtering is applied to all members, no validation.
Filter-Active - Filtering is applied to all members, validation is performed only for the active member.
Filter-Backup - Filtering is applied to all members, validation is performed only for backup members.
Type: Refer to - definitions->bonding->ARPValidate
Default: none

2.8.3.14.11 ARPAllTargets

Property: Links :: Interface :: Bonding :: ARPAllTargets
Item description: Specifies the quantity of ARPIPTargets that must be reachable in order for the ARP monitor to consider a member as being up. Consider the member up if any of the ARPIPTargets is reachable (false) or consider the member up only when all of the ARPIPTargets are reachable (true).
Item type: Boolean true or false.
Default: false

2.8.3.14.12 DownDelay

Property: Links :: Interface :: Bonding :: DownDelay

Item description: Specifies, in milliseconds, the amount of time to wait before disabling a member after a link failure has been detected. Only valid for MIIMon. DownDelay should be a multiple of the MIIMon value.
Item type: Integer with a minimum of 0.
Default: 0

2.8.3.14.13 FailoverMAC

Property: Links :: Interface :: Bonding :: FailoverMAC
Item description: Specifies whether or not Active-Backup mode should set all members to the same MAC address at time of bonding:
None - Disables FailoverMAC.
Active - The MAC address of the bond should always be the MAC address of the currently active member.
Follow - The MAC address of the bond is to be selected normally.
Type: Refer to - definitions->bonding->FailoverMAC
Default: none

2.8.3.14.14 LACPRate

Property: Links :: Interface :: Bonding :: LACPRate
Item description: Rate at which link partner is asked to transmit LACPDU packets in 802.3ad mode:
Slow - Transmit every 30 seconds.
Fast - Transmit every 1 second.
Type: Refer to - definitions->bonding->LACP
Default: slow

2.8.3.14.15 MaxBonds

Property: Links :: Interface :: Bonding :: MaxBonds
Item description: Number of bonding devices to create for this instance of the bonding driver.
Item type: Integer with a minimum of 0.
Default: 1

2.8.3.14.16 MIIMon

Property: Links :: Interface :: Bonding :: MIIMon
Item description: The MII link monitoring frequency in milliseconds. This determines how often the link state of each member is inspected for link failures. A value of 100 is a good starting point. 0 disables MII link monitoring.
Item type: Integer with a minimum of 0.
Default: 0

2.8.3.14.17 MinLinks

Property: Links :: Interface :: Bonding :: MinLinks
Item description: The minimum number of links that must be active before asserting carrier. Similar to the Cisco EtherChannel min-links feature. Only valid for 802.3ad mode.

Item type: Integer with a minimum of 0.
Default: 0

2.8.3.14.18 Mode

Property: Links :: Interface :: Bonding :: Mode
Item description: Specify one of the bonding policies:
Balance-RR - Transmit packets in order from first member to last. Provides load balancing and fault tolerance.
Active-Backup - Only one member is active. A different member becomes active if, and only if, the active member fails. Provides fault tolerance.
Balance-XOR - Transmit based on selected transmit hash policy. Provides load balancing and fault tolerance.
Broadcast - Transmit everything on all member interfaces. Provides fault tolerance.
802.3ad - Creates aggregation groups that share the same speed and duplex settings. Requires special switch support.
Balance-TLB - Adaptive transmit load balancing. Does not require special switch support.
Balance-ALB - Adaptive load balancing, includes Balance-TLB plus receive load balancing. Does not require special switch support.
Type: Refer to - definitions->bonding->Modes
Default: balance-rr

2.8.3.14.19 NumGratuitousARP

Property: Links :: Interface :: Bonding :: NumGratuitousARP
Item description: The number of peer notifications to be issued after a failover event. Only affects Active-Backup mode.
Item type: Integer with a minimum of 0 and a maximum of 255.
Default: 1

2.8.3.14.20 PacketsPerMember

Property: Links :: Interface :: Bonding :: PacketsPerMember
Item description: The number of packets to transmit though a member before moving to the next one. Only affects Balance-RR mode. When set to 0 a member is chosen at random.
Item type: Integer with a minimum of 0 and a maximum of 65535.
Default: 1

2.8.3.14.21 Primary

Property: Links :: Interface :: Bonding :: Primary
Item description: The interface name of the member which is the primary device. Useful when one member is preferred over another. Only valid for Active-Backup, Balance-TLB, and Balance-ALB modes.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.14.22 PrimaryReselect

Property: Links :: Interface :: Bonding :: PrimaryReselect
Item description: The reselection policy for the primary member. Determines how the primary member is chosen to become active when failure of the active member occurs.
Aways - The primary member becomes active whenever it is up.
Better - The primary member becomes active when it comes back up if the speed and duplex is better than the current active member.
Failure - The primary member becomes active only if the current active member fails.
Type: Refer to - definitions->bonding->PrimaryReselect
Default: always

TLBDynamicLoadBalancing
Property: Links :: Interface :: Bonding :: TLBDynamicLoadBalancing
Item description: Enables dynamic shuffling of flows. Only valid for Balance-TLB and Balance-ALB mode.
Item type: Boolean true or false.
Default: True

2.8.3.14.23 UpDelay

Property: Links :: Interface :: Bonding :: UpDelay
Item description: Milliseconds to wait before enabling a member after a link recovery has been detected. Only vlid for MIIMon link monitor. UpDelay value should be a multiple of the MIIMon value.
Item type: Integer with a minimum of 0.
Default: 0

2.8.3.14.24 XmitHashPolicy

Property: Links :: Interface :: Bonding :: XmitHashPolicy
Item description: Transmit has policy to use for member selection in Balance-XOR, 802.3ad, Balance-TLB, and Balance-ALB modes:
Layer2
Layer2+3
Layer3+4
Encap2+3
Encap3+4
Type: Refer to - definitions->bonding->XmitHashPolicy
Default: layer2

2.8.3.14.25 ResendIGMP

Property: Links :: Interface :: Bonding :: ResendIGMP
Item description: The number of IGMP membership reports to be issued after a failover event. This is useful for bonding modes Balance-RR, Active-Backup, Balance-TLB, and Balance-ALB in which a failover can switch IGMP traffic from one member to another.
Item type: Integer with a minimum of 0 and a maximum of 255.
Default: 1

2.8.3.14.26 LPInterval
Property: Links :: Interface :: Bonding :: LPInterval
Item description: number of seconds between instances where learning packets are sent to each member's peer switch. Only has effect in Balance-TLB and Balance-ALB modes.
Item type: Integer with a minimum of 1 and a maximum of 2147483647.
Default: 1

2.8.3.15 VETH
Property: Links :: Interface :: VETH
Item description: Configuration of a VETH interface.
Item type: JSON Object
Required: ['Peer']
Default: None

2.8.3.15.1 Peer
Property: Links :: Interface :: VETH :: Peer
Item description: The name of the peer interface that is automatically created to pair with this VETH interface.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.16 Bridge
Property: Links :: Interface :: Bridge
Item description: Configuration of a Bridge interface.
Item type: JSON Object
Default: None

2.8.3.16.1 Members
Property: Links :: Interface :: Bridge :: Members
Item description: The list of interfaces added to this bridge, these interfaces must already exist.
Item type: Array of unique items.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.17 TunTap
Property: Links :: Interface :: TunTap
Item description: Configuration of a TunTap interface.
Item type: JSON Object
Required: ['Mode']
Default: None

2.8.3.17.1 Mode
Property: Links :: Interface :: TunTap :: Mode
Item description: The mode of this device: tun=layer3, tap=layer2.

Item type: String enum of tun, tap.
Default: None

2.8.3.18 RoutableAddress

Property: Links :: Interface :: RoutableAddress
Item description: An additional IPv4 address to add to the interface which is used specifically for routing.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.8.3.19 WiFi

Property: Links :: Interface :: WiFi
Item description: Configure a wireless interface.
Item type: JSON Object
Default: None

2.8.3.19.1 Client

Property: Links :: Interface :: WiFi :: Client
Item description: Configuration of a Wifi client.
Item type: JSON Object
Required: ['SSID']
Default: None

2.8.3.19.1.1SSID

Property: Links :: Interface :: WiFi :: Client :: SSID
Item description: The SSID of the wireless network to connect to.
Type: Refer to - definitions->wlanmanager->wifi_ssid
Default: None

2.8.3.19.1.2Passphrase

Property: Links :: Interface :: WiFi :: Client :: Passphrase
Item description: The passphrase to connect to the wireless network. If ends in ".wpa2" it assumes the passphrase is read from a file with this name.
Type: Refer to - definitions->pki->passphrase_or_wpa2
Default:

2.8.3.19.1.3Timeout

Property: Links :: Interface :: WiFi :: Client :: Timeout
Item description: The number of seconds to wait to connect to the SSID before failing
Type: Refer to - definitions->types->UINT8
Default: 5

2.8.3.19.2 AccessPoints

Property: Links :: Interface :: WiFi :: AccessPoints

Item description: Configure a Wifi access points provided by this device
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item description: Configure a Wifi access point
Item type: JSON Object
Required: ['SSID']
Default: None

2.8.3.19.2.1SSID
Property: Links :: Interface :: WiFi :: AccessPoints :: SSID
Item description: The SSID of the access point.
Type: Refer to - definitions->wlanmanager->wifi_ssid
Default: None

2.8.3.19.2.2Standard
Property: Links :: Interface :: WiFi :: AccessPoints :: Standard
Item description: Default AP settings for a specific Wifi standard.
Item type: Enum of 802.11b, 802.11g, 802.11n_2.4, 802.11n_5, 802.11ac.
Default: 802.11n_5

2.8.3.19.2.3OperationMode
Property: Links :: Interface :: WiFi :: AccessPoints :: OperationMode
Item description: Operation mode (a = IEEE 802.11a (5 GHz), b = IEEE 802.11b (2.4 GHz), g = IEEE 802.11g (2.4 GHz), ad = IEEE 802.11ad (60 GHz); a/g options are used with IEEE 802.11n (HT), too, to specify band). Is automatically set by the Standard setting.
Item type: Enum of a, b, g, ad.
Default: None

2.8.3.19.2.4WMMEnabled
Property: Links :: Interface :: WiFi :: AccessPoints :: WMMEnabled
Item description: Enable WMM (IEEE 802.11 draft; 11-03-0504-03-000e) for 802.11a or 802.11g networks. Is automatically set by the Standard setting.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.5IEEE802.11n
Property: Links :: Interface :: WiFi :: AccessPoints :: IEEE802.11n
Item description: Whether IEEE 802.11n (HT) is enabled. Note: You will also need to enable WMM for full HT functionality. Is automatically set by the Standard setting.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.6RequireHT
Property: Links :: Interface :: WiFi :: AccessPoints :: RequireHT
Item description: Require stations to support HT PHY (reject association if they do not). Is automatically set by the Standard setting.
Item type: Boolean true or false.

Default: None

2.8.3.19.2.7IEEE802.11ac

Property: Links :: Interface :: WiFi :: AccessPoints :: IEEE802.11ac
Item description: Whether IEEE 802.11ac (VHT) is enabled. Note: You will also need to enable WMM for full VHT functionality. Is automatically set by the Standard setting.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.8RequireVHT

Property: Links :: Interface :: WiFi :: AccessPoints :: RequireVHT
Item description: Require stations to support VHT PHY (reject association if they do not). Is automatically set by the Standard setting.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.9Bridge

Property: Links :: Interface :: WiFi :: AccessPoints :: Bridge
Item description: In case of nl80211 driver interfaces, the bridge setting may be used to notify that the interface is included in a bridge. If the bridge parameter is not set, the drivers will automatically figure out the bridge interface and this parameter may not be needed. For nl80211, this parameter can be used to request the AP interface to be added to the bridge automatically. If needed, the bridge interface is also created.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.3.19.2.10 Driver

Property: Links :: Interface :: WiFi :: AccessPoints :: Driver
Item description: Driver interface type. "nl80211" is used with all Linux mac80211 drivers. Use "none" if building as a standalone RADIUS server that does not control any wireless/wired driver.
Item type: String enum of hostap, wired, none, nl80211, bsd.
Default: nl80211

2.8.3.19.2.11 LogLevel

Property: Links :: Interface :: WiFi :: AccessPoints :: LogLevel
Item description: The minimum value for logged events.
Item type: Enum of warning, notification, informational, debug, verbose.
Default: notification

2.8.3.19.2.12 CountryCode

Property: Links :: Interface :: WiFi :: AccessPoints :: CountryCode
Item description: Country code (ISO/IEC 3166-1). Used to set regulatory domain. Set as needed to indicate country in which device is operating. This can limit available channels and transmit power.
Item type: String pattern of ^[A-Z]{2}$.

Default: US

2.8.3.19.2.13 IEEE802.11d

Property: Links :: Interface :: WiFi :: AccessPoints :: IEEE802.11d
Item description: Enable IEEE 802.11d. This advertises the country code and the set of allowed channels and transmit power levels based on the regulatory limits.
Item type: Boolean true or false.
Default: False

2.8.3.19.2.14 IEEE802.11h

Property: Links :: Interface :: WiFi :: AccessPoints :: IEEE802.11h
Item description: Enable IEEE 802.11h. This enables radar detection and DFS support if available. DFS support is required on outdoor 5GHz channels in most countries. This can be used only with 802.11d enabled.
Item type: Boolean true or false.
Default: False

2.8.3.19.2.15 PowerConstraint

Property: Links :: Interface :: WiFi :: AccessPoints :: PowerConstraint
Item description: Add Power Constraint element to Beacon and Probe Response frames. This config option adds Power Constraint element when applicable and Country element is added. Power Constraint element is required by Transmit Power Control. This can be used only with 802.11d enabled. Valid values are 0-255.
Type: Refer to - definitions->types->UINT8
Default: None

2.8.3.19.2.16 SpectrumManagement

Property: Links :: Interface :: WiFi :: AccessPoints :: SpectrumManagement
Item description: Set Spectrum Management subfield in the Capability Information field. This config option forces the Spectrum Management bit to be set. When this option is not set, the value of the Spectrum Management bit depends on whether DFS or TPC is required by regulatory authorities. This can be used only with IEEE802.11d enabled and PowerConstraint configured.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.17 Channel

Property: Links :: Interface :: WiFi :: AccessPoints :: Channel
Item description: The channel number
Type: Refer to - definitions->wlanmanager->channelorauto
Default: auto

2.8.3.19.2.18 GlobalOperatingClass

Property: Links :: Interface :: WiFi :: AccessPoints :: GlobalOperatingClass

Item description: This option allows hostapd to specify the operating class of the channel configured with the channel parameter. channel and op_class together can uniquely identify channels across different bands, including the 6 GHz band.
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.8.3.19.2.19 ACS

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS
Item description: Tuning parameters for Automatic Channel Selection (ACS).
Item type: JSON Object
Default: None

2.8.3.19.2.19.1 NumScans

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: NumScans
Item description: The number of scans performed for ACS.
Item type: Integer with a minimum of 1 and a maximum of 100.
Default: None

2.8.3.19.2.19.2 ChannelBias

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: ChannelBias
Item description: Increase or decrease the likelihood of a specific channel to be selected by the ACS algorithm. Bias 0.0-1.0 make the channel more likely to be picked while values >1.0 make it less likely.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item description: Define a channel bias for specific channels to increase/decrease the likelihood of a specific channel to be selected by the ACS algorithm. Bias < 1.0 increases the likelihood a channel is used.
Item type: JSON Object
Required: ['channel', 'bias']
Default: None

2.8.3.19.2.19.2.1 channel

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: ChannelBias :: channel
Type: Refer to - definitions->wlanmanager->channel
Default: None

2.8.3.19.2.19.2.2 bias

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: ChannelBias :: bias
Item type: Number.
Default: None

2.8.3.19.2.19.3 ChannelList

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: ChannelList

Item description: Channel list restriction. This option selects one of these channels when a channel should be automatically selected.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->wlanmanager->channel
Default: None

2.8.3.19.2.19.4ExcludeDFS

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: ExcludeDFS
Item description: If set, exclude DFS channels from ACS
Item type: Boolean true or false.
Default: None

2.8.3.19.2.19.5Exclude6ghzNonPSC

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: Exclude6ghzNonPSC
Item description: If set, include only preferred scan channels from 6GHz band for ACS.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.19.6MinTXPower

Property: Links :: Interface :: WiFi :: AccessPoints :: ACS :: MinTXPower
Item description: Set minimum permitted max TX power (in dBm) for ACS and DFS channel selection.
Type: Refer to - definitions->types->UINT8
Default: None

2.8.3.19.2.20 BeaconInterval

Property: Links :: Interface :: WiFi :: AccessPoints :: BeaconInterval
Item description: Beacon interval in kus (1.024 ms) (15..65535)
Item type: Integer with a minimum of 15 and a maximum of 65535.
Default: None

2.8.3.19.2.21 DTIMPeriod

Property: Links :: Interface :: WiFi :: AccessPoints :: DTIMPeriod
Item description: DTIM (delivery traffic information message) period (1..255). I.E. number of beacons between DTIMs (1 = every beacon includes DTIM element)
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.8.3.19.2.22 MaxStations

Property: Links :: Interface :: WiFi :: AccessPoints :: MaxStations
Item description: Maximum number of stations allowed in station table. New stations will be rejected after the station table is full. IEEE 802.11 has a limit of 2007 different association IDs, so this number should not be larger than that.
Item type: Integer with a minimum of 1 and a maximum of 2007.
Default: None

2.8.3.19.2.23 RTSThreshold

Property: Links :: Interface :: WiFi :: AccessPoints :: RTSThreshold
Item description: RTS/CTS threshold (0-2347, 2347 = disabled). If this field is not included the RTS threshold will not be controlled.
Item type: Integer with a minimum of 0 and a maximum of 65535.
Default: None

2.8.3.19.2.24 FragmentationThreshold

Property: Links :: Interface :: WiFi :: AccessPoints :: FragmentationThreshold
Item description: Fragmentation threshold (256-2346, 2346 = disabled). If this field is not included the fragmentation threshold will not be controlled.
Item type: Integer with a minimum of 256 and a maximum of 2346.
Default: None

2.8.3.19.2.25 ShortPreamble

Property: Links :: Interface :: WiFi :: AccessPoints :: ShortPreamble
Item description: Enable optional use of short preamble for frames sent at 2 Mbps, 5.5 Mbps, and 11 Mbps to improve network performance.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.26 BroadcastSSID

Property: Links :: Interface :: WiFi :: AccessPoints :: BroadcastSSID
Item description: Enable/disable broadcasting the SSID.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.27 Multicast2Unicast

Property: Links :: Interface :: WiFi :: AccessPoints :: Multicast2Unicast
Item description: Request that the AP will do multicast-to-unicast conversion for ARP, IPv4, and IPv6 frames (possibly within 802.1Q). If enabled, such frames are to be sent to each station separately, with the DA replaced by their own MAC address rather than the group address. Note that this may break certain expectations of the receiver
Item type: Boolean true or false.
Default: None

2.8.3.19.2.28 Authentication

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication
Item description: Configure out clients authenticate with the access point
Item type: JSON Object
Default: None

2.8.3.19.2.28.1 WPA

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: WPA
Item description: Enable WPA. 0=disabled, 1=WPA, 2=WPA2/3, 3=WPA and WPA2/3

Item type: Enum of 0, 1, 2, 3.
Default: None

2.8.3.19.2.28.2 WPAKeyManagement

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: WPAKeyManagement
Item description: Set of accepted key management algorithms.
WPA-PSK = WPA-Personal / WPA2-Personal
WPA-PSK-SHA256 = WPA2-Personal using SHA256
WPA-EAP = WPA-Enterprise / WPA2-Enterprise
WPA-EAP-SHA256 = WPA2-Enterprise using SHA256
SAE = SAE (WPA3-Personal)
WPA-EAP-SUITE-B-192 = WPA3-Enterprise with 192-bit security/CNSA suite
FT-PSK = FT with passphrase/PSK
FT-EAP = FT with EAP
FT-EAP-SHA384 = FT with EAP using SHA384
FT-SAE = FT with SAE
FILS-SHA256 = Fast Initial Link Setup with SHA256
FILS-SHA384 = Fast Initial Link Setup with SHA384
FT-FILS-SHA256 = FT and Fast Initial Link Setup with SHA256
FT-FILS-SHA384 = FT and Fast Initial Link Setup with SHA384
OWE = Opportunistic Wireless Encryption (a.k.a. Enhanced Open)
DPP = Device Provisioning Protocol
OSEN = Hotspot 2.0 online signup with encryption
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of WPA-PSK, WPA-PSK-SHA256, WPA-EAP, WPA-EAP-SHA256, SAE, WPA-EAP-SUITE-B-192, FT-PSK, FT-EAP, FT-EAP-SHA384, FT-SAE, FILS-SHA256, FILS-SHA384, FT-FILS-SHA256, FT-FILS-SHA384, OWE, DPP, OSEN.
Default: None

2.8.3.19.2.28.3 WPAPairwise

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: WPAPairwise
Item description: Set of accepted cipher suites for pairwise keys for WPA. If not set, defaults to TKIP.
TKIP = Temporal Key Integrity Protocol
CCMP = AES in Counter Mode with CBC-MAC
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of TKIP, CCMP.
Default: None

2.8.3.19.2.28.4 RSNPairwise

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: RSNPairwise
Item description: Set of accepted cipher suites for pairwise keys for RSN/WPA2. If not set, defaults to WPAPairwise value.
TKIP = Temporal Key Integrity Protocol
CCMP = AES in Counter Mode with CBC-MAC

Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of TKIP, CCMP.
Default: None

2.8.3.19.2.28.5Passphrase

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: Passphrase
Item description: The passphrase to connect to the wireless network. If ends in ".wpa2" it assumes the passphrase is read from a file with this name.
Type: Refer to - definitions->pki->passphrase_or_wpa2
Default: None

2.8.3.19.2.28.6ACL

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: ACL
Item description: Enabled station MAC address based authentication. allow=allow unless in deny list, deny=deny unless in allow list, radius=use external RADIUS server (allow/deny lists are searched first)
Item type: Enum of allow, deny, radius.
Default: None

2.8.3.19.2.28.7AllowList

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: AllowList
Item description: List of allowed client MAC Addresses. If specified, this list is used regardless of deny list configuration. If not specified, use deny list, if specified, otherwise all clients will be allowed.
Type: Refer to - definitions->types->HardwareAddressArr
Default: None

2.8.3.19.2.28.8DenyList

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: DenyList
Item description: List of denied client MAC Addresses. If specified, and allow list is not specified, allow all clients except those in this list. If not specified, default to the allow list. If neither is set, allow all.
Type: Refer to - definitions->types->HardwareAddressArr
Default: None

2.8.3.19.2.28.9IEEE8021x

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: IEEE8021x
Item description: Require IEEE 802.1X authorization.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.28.10 EAPOLVersion

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: EAPOLVersion

Item description: IEEE 802.1X/EAPOL version.
Item type: Enum of 1, 2, 3.
Default: None

2.8.3.19.2.28.11 EAPServer

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: EAPServer
Item description: Use integrated EAP server instead of external RADIUS authentication server.
Item type: Boolean true or false.
Default: None

2.8.3.19.2.28.12 EAPUserFile

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: EAPUserFile
Item description: Path for EAP server user database.
Type: Refer to - definitions->pki->file
Default: None

2.8.3.19.2.28.13 CACert

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: CACert
Item description: CA certificate (PEM or DER file) for EAP-TLS/PEAP/TTLS.
Type: Refer to - definitions->pki->file
Default: None

2.8.3.19.2.28.14 ServerCert

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: ServerCert
Item description: Server certificate (PEM or DER file) for EAP-TLS/PEAP/TTLS.
Type: Refer to - definitions->pki->file
Default: None

2.8.3.19.2.28.15 PrivateKey

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: PrivateKey
Item description: Private key matching with the server certificate for EAP-TLS/PEAP/TTLS.
Type: Refer to - definitions->pki->file
Default: None

2.8.3.19.2.28.16 OwnIPAddr

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: OwnIPAddr
Item description: The own IP address of the access point (used as NAS-IP-Address).
Type: Refer to - definitions->types->IPAddress
Default: None

2.8.3.19.2.28.17 RADIUSAuthServerIP

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: RADIUSAuthServerIP
Item description: RADIUS authentication server IP Address

Type: Refer to - definitions->types->IPAddress
Default: None

2.8.3.19.2.28.18 RADIUSAuthServerPort

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: RADIUSAuthServerPort
Item description: RADIUS authentication server port
Type: Refer to - definitions->types->Port
Default: None

2.8.3.19.2.28.19 RADIUSAuthServerSecret

Property: Links :: Interface :: WiFi :: AccessPoints :: Authentication :: RADIUSAuthServerSecret
Item description: RADIUS authentication server shared secret. If ends in ".pass" it assumes the secret is read from a file with this name.
Type: Refer to - definitions->pki->password_or_pass
Default: None

2.8.3.19.2.29 ExtraConfig

Property: Links :: Interface :: WiFi :: AccessPoints :: ExtraConfig
Item description: Additional "<key>=<value>" pairs for hostapd that may not have been explicitly defined here. These options are all written to the end of the hostapd config file and may override earlier settings.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String.
Default: None

2.8.3.20 DHCP

Property: Links :: Interface :: DHCP
Item description: Configuration for running a DHCPv4/v6 server on this interface.
Item type: JSON Object
Default: None

2.8.3.20.1 IPv4

Property: Links :: Interface :: DHCP :: IPv4
Item description: Configuration of the DHCPv4 server.
Item type: JSON Object
Default: None

2.8.3.20.1.1Enable

Property: Links :: Interface :: DHCP :: IPv4 :: Enable
Item description: Enable the DHCPv4 server on this interface. If no subnets or pools are manually configured, a DHCP pool will be automatically generated based on the interface address.
Item type: Boolean true or false.

Default: False

2.8.3.20.1.2Subnet4

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4
Item description: A list of DHCPv4 subnets to configure.
Item type: Array of unique items and a minimum number of 1 item(s).
Item description: Configuration of a single DHCPv4 subnet.
Item type: JSON Object
Required: ['Subnet', 'Pools']
Default: None

2.8.3.20.1.2.1 Subnet

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Subnet
Item description: The subnet to configure DHCP on (CIDR notation).
Item type: String.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.8.3.20.1.2.2 ID

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: ID
Item description: The subnet ID (UINT32). Manually setting subnet IDs may help avoid issues when removing subnets. If not set, subnets will be numbered in sequence starting at 1. Setting to 0 forces this auto-generation of subnet IDs.
Type: Refer to - definitions->types->UINT32
Default: None

2.8.3.20.1.3Pools

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Pools
Item description: The pools of IP addresses in the subnet that should be made available for distribution.
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Required: ['Pool']
Default: None

2.8.3.20.1.3.1.1 Pool

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Pools :: Pool
Item description: A range of IP addresses in the form "192.0.0.0-192.0.0.127".
Type: Refer to - definitions->types->DottedQuadRange
Or
Item description: A range of IP addresses in CIDR notation: "192.0.0.0/25".
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.8.3.20.1.3.1.2 OptionData

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Pools :: OptionData
Item description: Standard DHCPv4 options; options set at the pool level override global and subnet settings.
Type: Refer to - definitions->dhcp->OptionData4
Default: None

2.8.3.20.1.3.2 ValidLifetime

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: ValidLifetime
Item description: The default lease time in seconds used if the client does not request a specific lease. Default to one hour.
Item type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 3600

2.8.3.20.1.3.3 MaxValidLifetime

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: MaxValidLifetime
Item description: The longest lease time the server can allocate. Default to one day.
Item type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 86400

2.8.3.20.1.3.4 Reservations

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Reservations
Item type: Array of unique items.
Item type: JSON Object
Default: None

2.8.3.20.1.3.4.1 HardwareAddress

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Reservations :: HardwareAddress
Item description: MAC address used to identify the client to create a reservation for.
Type: Refer to - definitions->types->HardwareAddress
Default: None

2.8.3.20.1.3.4.2 IpAddress

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Reservations :: IpAddress
Item description: Fixed IP address to issue to the client.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.3.20.1.3.4.3 Hostname

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Reservations :: Hostname
Item description: Fixed hostname to set for the client.
Item type: String pattern of ^[a-zA-Z0-9.-]+$.
Default: None

2.8.3.20.1.3.4.4 OptionData

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: Reservations :: OptionData
Item description: Standard DHCPv4 options; options set at the host level override global, subnet, and pool settings.
Type: Refer to - definitions->dhcp->OptionData4
Default: None

2.8.3.20.1.3.5 OptionData

Property: Links :: Interface :: DHCP :: IPv4 :: Subnet4 :: OptionData
Item description: Standard DHCPv4 options; options set at the subnet level override global settings.
Type: Refer to - definitions->dhcp->OptionData4
Default: None

2.8.3.20.2 IPv6

Property: Links :: Interface :: DHCP :: IPv6
Item description: Configuration of the DHCPv6 server.
Item type: JSON Object
Default: None

2.8.3.20.2.1Enable

Property: Links :: Interface :: DHCP :: IPv6 :: Enable
Item description: Enable the DHCPv6 server on this interface. If no subnets or pools are manually configured, a DHCP pool will be automatically generated based on the interface address.
Item type: Boolean true or false.
Default: False

2.8.3.20.2.2Subnet6

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6
Item description: A list of DHCPv6 subnets to configure.
Item type: Array of unique items and a minimum number of 1 item(s).
Item description: Configuration of a single DHCPv6 subnet.
Item type: JSON Object
Required: ['Subnet', 'Pools']
Default: None

2.8.3.20.2.2.1 Subnet

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Subnet
Item description: The subnet to configure DHCP on (CIDR notation).
Item type: String.
Type: Refer to - definitions->types->IPv6MaskReq
Default: None

2.8.3.20.2.2.2 ID

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: ID
Item description: The subnet ID (UINT32). Manually setting subnet IDs may help avoid issues when removing subnets. If not set, subnets will be numbered in sequence starting at 1. Setting to 0 forces this auto-generation of subnet IDs.
Type: Refer to - definitions->types->UINT32
Default: None

2.8.3.20.2.2.3 Pools

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Pools
Item description: The pools of IP addresses in the subnet that should be made available for distribution.
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Required: ['Pool']
Default: None

2.8.3.20.2.2.3.1 Pool

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Pools :: Pool
Item description: A range of IPv6 addresses in the form "min-max".
Type: Refer to - definitions->types->IPv6Range
Or
Item description: A range of IPv6 addresses in CIDR notation: "2001:db8:1::/64".
Type: Refer to - definitions->types->IPv6MaskReq
Default: None

2.8.3.20.2.2.3.2 OptionData

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Pools :: OptionData
Item description: Standard DHCPv6 options; options set at the pool level override global and subnet settings.
Type: Refer to - definitions->dhcp->OptionData6
Default: None

2.8.3.20.2.2.4 ValidLifetime

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: ValidLifetime
Item description: The default lease time in seconds used if the client does not request a specific lease. Default to one hour.
Item type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 3600

2.8.3.20.2.2.5 MaxValidLifetime

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: MaxValidLifetime
Item description: The longest lease time the server can allocate. Default to one day.
Item type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 86400

2.8.3.20.2.2.6 Reservations

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Reservations
Item type: Array of unique items.
Item type: JSON Object
Default: None

2.8.3.20.2.2.6.1 HardwareAddress

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Reservations :: HardwareAddress
Item description: MAC address used to identify the client to create a reservation for.
Type: Refer to - definitions->types->HardwareAddress
Default: None

2.8.3.20.2.2.6.2 DUID

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Reservations :: DUID
Item description: DHCPv6 Unique Identifier (DUID) used to identify the client to create a reservation for.
Type: Refer to - definitions->types->DUID
Default: None

2.8.3.20.2.2.6.3 IpAddress

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Reservations :: IpAddress
Item description: Fixed IPv6 address to issue to the client.
Type: Refer to - definitions->types->IPv6Address
Default: None

2.8.3.20.2.2.6.4 Hostname

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Reservations :: Hostname
Item description: Fixed hostname to set for the client.
Item type: String pattern of ^[a-zA-Z0-9.-]+$.
Default: None

2.8.3.20.2.2.6.5 OptionData

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: Reservations :: OptionData
Item description: Standard DHCPv6 options; options set at the host level override global, subnet, and pool settings.
Type: Refer to - definitions->dhcp->OptionData6
Default: None

2.8.3.20.2.2.7 OptionData

Property: Links :: Interface :: DHCP :: IPv6 :: Subnet6 :: OptionData
Item description: Standard DHCPv6 options; options set at the subnet level override global settings.
Type: Refer to - definitions->dhcp->OptionData6

Default: None

2.8.3.21 Sysctl

Property: Links :: Interface :: Sysctl
Item description: Interface-specific sysctl configuration; used to modify kernel parameters at runtime.
Item type: JSON Object
Default: None

2.8.3.21.1 Net

Property: Links :: Interface :: Sysctl :: Net
Item description: Network-related kernel parameters.
Item type: JSON Object
Default: None

2.8.3.21.1.1IPv4

Property: Links :: Interface :: Sysctl :: Net :: IPv4
Item description: IPv4 parameters.
Item type: JSON Object
Default: None

2.8.3.21.1.1.1 Conf

Property: Links :: Interface :: Sysctl :: Net :: IPv4 :: Conf
Item description: IPv4 configuration parameters.
Type: Refer to - definitions->Sysctl->Net->IPv4->Conf
Default: None

2.8.3.21.1.2IPv6

Property: Links :: Interface :: Sysctl :: Net :: IPv6
Item description: IPv6 parameters.
Item type: JSON Object
Default: None

2.8.3.21.1.2.1 Conf

Property: Links :: Interface :: Sysctl :: Net :: IPv6 :: Conf
Item description: IPv6 configuration parameters.
Type: Refer to - definitions->Sysctl->Net->IPv6->Conf
Default: None

2.8.4 Actions

Property: Links :: Actions
Item description: Configuration of actions (system commands) to run triggered by various events on this link.
Item type: JSON Object

Default: None

2.8.4.1 Up

Property: Links :: Actions :: Up
Item description: Action to take when the link comes up. (Interface is found, configured, and brought up)
Item type: String.
Default: None

2.8.4.2 Down

Property: Links :: Actions :: Down
Item description: Action to take when the link goes down. (Either interface disappeared and link is reset, or during shutdown and link is cleaning up)
Item type: String.
Default: None

2.8.5 Parent

Property: Links :: Parent
Item description: Set a controlling parent device for this interface. Such as adding to a bridge or VRF. Can be an interface name, or ARES link name.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.8.6 Routes

Property: Links :: Routes
Item description: Array of static routes for both IPv4 and IPv6 reachable through this link.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->staticroutes->RouteObject
Default: None

2.8.7 OSPF

Property: Links :: OSPF
Item description: OSPF configuration of this link which overrides the default configuration.
Item type: JSON Object
Default: None

2.8.7.1 Area

Property: Links :: OSPF :: Area
Item description: The OSPF area used for this link. Overrides the global configuration. Default: Global configuration
Type: Refer to - definitions->ospf->OSPFArea
Default: None

2.8.7.2 Authentication
Property: Links :: OSPF :: Authentication
Item description: Configuration of the OSPF message authentication on this link
Type: Refer to - definitions->ospf->OSPFAuthentication
Default: None

2.8.7.3 Advertise
Property: Links :: OSPF :: Advertise
Item description: Announce this link to the network via OSPF.
Item type: Boolean true or false.
Default: True

2.8.7.4 DefaultGateway
Property: Links :: OSPF :: DefaultGateway
Item description: The gateway address used for the default route on this link. It will automatically be advertised.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.7.5 Passive
Property: Links :: OSPF :: Passive
Item description: Mark this interface as passive so that it doesn't perform OSPF neighbor discovery.
Item type: Boolean true or false.
Default: True

2.8.8 Multicast
Property: Links :: Multicast
Item description: The interface specific multicast configuration for this link.
Item type: JSON Object
Default: None

2.8.8.1 Enabled
Property: Links :: Multicast :: Enabled
Item description: Enable/disable IGMP and PIM on this link.
Item type: Boolean true or false.
Default: False

2.8.8.2 UnprotectedStaticRanges
Property: Links :: Multicast :: UnprotectedStaticRanges
Item description: Enable/disable(default) automatic global forwarding of ranged static multicast routes within the protected range (224.0.0.0/24).
Item type: Boolean true or false.
Default: False

2.8.8.3 IGMP

Property: Links :: Multicast :: IGMP
Item description: Link IGMP configuration.
Item type: JSON Object
Default: None

2.8.8.3.1 Version

Property: Links :: Multicast :: IGMP :: Version
Item description: The IGMP version to use on this link.
Item type: Integer enum of 2, 3.
Default: 3

2.8.8.3.2 Query-Interval

Property: Links :: Multicast :: IGMP :: Query-Interval
Item description: Time, in seconds, between sending IGMP General Query messages.
Item type: Integer with a minimum of 1 and a maximum of 1800.
Default: 125

2.8.8.3.3 Query-Max-Response-Time

Property: Links :: Multicast :: IGMP :: Query-Max-Response-Time
Item description: Maximum time, in deci-seconds, that a receiver has to respond to a query.
Item type: Integer with a minimum of 10 and a maximum of 250.
Default: 10

2.8.8.3.4 Last-Member-Query-Count

Property: Links :: Multicast :: IGMP :: Last-Member-Query-Count
Item description: Number of group queries to send when the last members leaves the group.
Item type: Integer with a minimum of 1 and a maximum of 7.
Default: 2

2.8.8.3.5 Last-Member-Query-Interval

Property: Links :: Multicast :: IGMP :: Last-Member-Query-Interval
Item description: Time, in deci-seconds, between sending last member queries.
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: 10

2.8.8.3.6 Static-Joins

Property: Links :: Multicast :: IGMP :: Static-Joins
Item description: Static IGMP joins for this interface, as if received from a different host on this interface. Useful when dealing with hosts that don't support IGMP but want to receive multicast traffic.
Item type: Array with a minimum number of 1 item(s) that must be unique.

Item type: JSON Object
Required: ['Group']
Default: None

2.8.8.3.6.1 Group

Property: Links :: Multicast :: IGMP :: Static-Joins :: Group
Item description: The group to join.
Type: Refer to - definitions->types->IPv4Multicast
Default: None

2.8.8.3.6.2 Source

Property: Links :: Multicast :: IGMP :: Static-Joins :: Source
Item description: The source to receive from.
Type: Refer to - definitions->types->IPv4Address
Or
Type: Refer to - definitions->types->IPv4Multicast
Default: None

2.8.8.4 PIM

Property: Links :: Multicast :: PIM
Item description: Link PIM configuration.
Item type: JSON Object
Default: None

2.8.8.4.1 BFD

Property: Links :: Multicast :: PIM :: BFD
Item description: A detection protocol designed to provide fast forwarding path failure detection times. Overrides global configuration.
Item type: Boolean true or false.
Default: None

2.8.8.4.2 BSM

Property: Links :: Multicast :: PIM :: BSM
Item description: Allows an interface to process bootstrap messages. Overrides global configuration.
Item type: Boolean true or false.
Default: None

2.8.8.4.3 Unicast-BSM

Property: Links :: Multicast :: PIM :: Unicast-BSM
Item description: Allows an interface to process unicast bootstrap messages. Overrides global configuration.
Item type: Boolean true or false.
Default: None

2.8.8.4.4 DR-Priority
Property: Links :: Multicast :: PIM :: DR-Priority
Item description: The priority level used to influence DR election per-link. Overrides global configuration.
Item type: Integer with a minimum of 1 and a maximum of 4294967295.
Default: None

2.8.8.4.5 Hello-Interval
Property: Links :: Multicast :: PIM :: Hello-Interval
Item description: The time, in seconds, between sending PIM hello messages. Overrides global configuration.
Item type: Integer with a minimum of 1 and a maximum of 180.
Default: None

2.8.8.4.6 Boundary-List
Property: Links :: Multicast :: PIM :: Boundary-List
Item description: If a PIM join or IGMP report is received and the Group is defined here, PIM will ignore the join or report. Overrides global configuration.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Default: None

2.8.8.4.7 Use-Source
Property: Links :: Multicast :: PIM :: Use-Source
Item description: For multi-homed interfaces, choose the specific address to use as the source for PIM packets.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.8.5 Routes
Property: Links :: Multicast :: Routes
Item description: Static multicast routes.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: JSON Object
Required: ['Outgoing', 'Group']
Default: None

2.8.8.5.1 Outgoing
Property: Links :: Multicast :: Routes :: Outgoing
Item description: List of outgoing interfaces to send the multicast traffic on. They must have multicast enabled to be used in the multicast route.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->InterfaceName

Default: None

2.8.8.5.2 Group
Property: Links :: Multicast :: Routes :: Group
Type: Refer to - definitions->types->IPv4MulticastMaskOpt
Default: None

2.8.8.5.3 Source
Property: Links :: Multicast :: Routes :: Source
Type: Refer to - definitions->types->IPv4MaskOpt
Default: None

2.8.9 EnableNAT
Property: Links :: EnableNAT
Item description: Perform source NATing on this interface. Disabled by default unless it is a WAN link.
Item type: Boolean true or false.
Default: False

2.8.10 PreserveDSCP
Property: Links :: PreserveDSCP
Item description: Original DSCP value is preserved through encapsulation. Required for networks that force a specific DSCP value.
Item type: Boolean true or false.
Default: False

2.8.11 NextHop
Property: Links :: NextHop
Item description: In cases where the endpoints on the link are in different subnets then an encapsulating routable address is configured and a next hop may need to be set to route traffic through the local endpoint.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.8.12 Quality
Property: Links :: Quality
Item description: Configuration of link quality parameters. By default, quality metrics will be automatically measured to each neighbor on a link with no bias, and probe measurements will automatically adjust based on the link bandwidth.
Item type: JSON Object
Default: None

2.8.12.1 Bias

Property: Links :: Quality :: Bias
Item description: Bias applied during quality calculations to fine tune the quality of this link.
Item type: Integer with a minimum of -30000 and a maximum of 30000.
Default: 0

2.8.12.2 Threshold
Property: Links :: Quality :: Threshold
Item description: Amount that the metric must change before it is applied to OSPF.
Type: Refer to - definitions->types->UINT16
Default: 25

2.8.12.3 Bandwidth
Property: Links :: Quality :: Bandwidth
Item description: Static bandwidth for this link, in bits/s. Setting a static value inhibits automatic measuring of the link bandwidth.
Item type: Integer with a minimum of 1 and a maximum of 4294967295.
Default: None

2.8.12.4 MaxBandwidth
Property: Links :: Quality :: MaxBandwidth
Item description: The maximum bandwidth, in bits/s, through this link for traffic to all of the neighbors on the link, which may be higher than any individual bandwidth measured to a neighbor. If not set, the highest measured value to a neighbor will be used. If static bandwidth is set, then max defaults to the same as the static bandwidth. The max bandwidth may be overwritten if there is a higher measured bandwidth.
Item type: Integer with a minimum of 1 and a maximum of 4294967295.
Default: None

2.8.12.5 BandwidthFloor
Property: Links :: Quality :: BandwidthFloor
Item description: The lowest possible bandwidth value, in bits/s, used for traffic control. If a measured bandwidth is less than this value, this value is used instead.
Item type: Integer with a minimum of 1 and a maximum of 4294967295.
Default: 100000

2.8.12.6 Latency
Property: Links :: Quality :: Latency
Item description: Static latency for this link, in ms. Setting a static value inhibits the automatic measuring of the link latency.
Item type: Integer with a minimum of 1 and a maximum of 600000.
Default: None

2.8.12.7 PacketLoss
Property: Links :: Quality :: PacketLoss

Item description: Static packet loss for this link, in percent. Setting a static value inhibits automatic measuring of the link packet loss.
Type: Refer to - definitions->types->Percentage
Default: None

2.8.12.8 PacketLossInterval

Property: Links :: Quality :: PacketLossInterval
Item description: The time, in seconds, between reporting packet loss measurements.
Item type: Integer.
Default: 60

2.8.12.9 PacketLossWindow

Property: Links :: Quality :: PacketLossWindow
Item description: The number of packets received after a missed packet before marking that missed packet as lost.
Item type: Integer.
Default: 25

2.8.12.10 ProbePort

Property: Links :: Quality :: ProbePort
Item description: The port number used by probe packets when measuring bandwidth/latency.
Type: Refer to - definitions->types->Port
Default: 32768

2.8.12.11 ProbeTTL

Property: Links :: Quality :: ProbeTTL
Item description: The TTL value used by probe packets when measuring bandwidth/latency. Must be high enough to reach the ARES neighbor at the end of the link.
Type: Refer to - definitions->types->TTL
Default: 30

2.8.12.12 ProbeLength

Property: Links :: Quality :: ProbeLength
Item description: The data size (not including headers) of the probe packets sent when measuring bandwidth/latency.
Item type: Integer with a minimum of 1 and a maximum of 1454.
Default: 1400

2.8.12.13 NumProbePackets

Property: Links :: Quality :: NumProbePackets
Item description: The number of probe packets sent when measuring bandwidth/latency. Default value of this and ProbeLength will generate ~500Kbps of traffic.
Item type: Integer with a minimum of 1 and a maximum of 65535.
Default: 45

2.8.12.14 ProbeTimeout

Property: Links :: Quality :: ProbeTimeout
Item description: The time, in milliseconds, to wait for the complete probe packet train to be received before timing out and using the incomplete data. This must be less than the Probe Interval and the Probe Report Timeout.
Item type: Integer with a minimum of 500 and a maximum of 10000.
Default: 2000

2.8.12.15 ProbeReportTimeout

Property: Links :: Quality :: ProbeReportTimeout
Item description: The time, in seconds, to wait for the bandwidth report before retesting with a smaller packet train. This must be greater than the Probe Timeout and less than the Probe Interval.
Item type: Integer with a minimum of 2 and a maximum of 10.
Default: 5

2.8.12.16 ProbeInterval

Property: Links :: Quality :: ProbeInterval
Item description: The time, in seconds, between taking probe measurements. This must be higher than the Probe Timeout and the Probe Report Timeout.
Item type: Integer with a minimum of 10 and a maximum of 600.
Default: 30

2.8.12.17 ProbeLimit

Property: Links :: Quality :: ProbeLimit
Item description: The percentage of probe packets that must be received in order to consider a bandwidth test valid. If there are too many dropped packets, the test is ignored.
Item type: Integer with a minimum of 40 and a maximum of 100.
Default: 75

2.8.12.18 AutoProbeAdjust

Property: Links :: Quality :: AutoProbeAdjust
Item description: If this flag is set, the probe algorithm will be automatically adjusted based off the previous calculation.
Item type: Boolean true or false.
Default: True

2.8.12.19 AutoProbePercent

Property: Links :: Quality :: AutoProbePercent
Item description: If the AutoProbeAdjust flag is set, this value is used to determine the amount of data to send as a percentage amount of the previous bandwidth measurement.
Item type: Integer with a minimum of 1 and a maximum of 50.
Default: 30

2.8.12.20 ShapingQueueSize

Property: Links :: Quality :: ShapingQueueSize
Item description: The size of the packet queue used in the traffic shaping. A larger queue size provides higher latency but less packet loss at the expense of increased memory usage.
Item type: Integer with a minimum of 0 and a maximum of 10000.
Default: 500

2.8.13 NeighborDiscovery

Property: Links :: NeighborDiscovery
Item description: Configuration of neighbor discovery protocol on this link.
Item type: JSON Object
Default: None

2.8.13.1 BootstrapRouter

Property: Links :: NeighborDiscovery :: BootstrapRouter
Item description: The IPv4 address of the Neighbor Discovery Bootstrap router on this link. Required if the link network does not support multicast.
Type: Refer to - definitions->types->IPv4Address
Default: 0.0.0.0

2.8.13.2 Group

Property: Links :: NeighborDiscovery :: Group
Item description: The multicast destination address to use when sending/receiving discovery messages.
Type: Refer to - definitions->types->IPv4Multicast
Default: 224.0.1.120

2.8.13.3 Port

Property: Links :: NeighborDiscovery :: Port
Item description: The port to use when sending/receiving discovery messages.
Type: Refer to - definitions->types->Port
Default: 12345

2.8.13.4 TTL

Property: Links :: NeighborDiscovery :: TTL
Item description: The TTL value used when sending discovery messages. Must be high enough to reach all neighbors on the link. Default 6(SRW, ANW2, TTNT), 20(LTE), 1(all others).
Type: Refer to - definitions->types->TTL
Default: 1

2.8.13.5 Interval

Property: Links :: NeighborDiscovery :: Interval

Item description: The time, in seconds, between sending discovery messages on this link.
Item type: Integer with a minimum of 1 and a maximum of 600.
Default: 5

2.8.13.6 Timeout

Property: Links :: NeighborDiscovery :: Timeout
Item description: Time, in seconds, without receiving a discovery message before considering a neighbor invalid. This value must be at least as long as the Interval.
Item type: Integer with a minimum of 1 and a maximum of 1200.
Default: 20

2.8.14 ZOOM

Property: Links :: ZOOM
Item description: Configuration of the ZOOM parameters for this interface.
Item type: JSON Object
Required: ['Enable']
Default: None

2.8.14.1 Enable

Property: Links :: ZOOM :: Enable
Item description: Enable ZOOM encoding on this interface.
Item type: Boolean true or false.
Default: False

2.8.14.2 AssumedTTL

Property: Links :: ZOOM :: AssumedTTL
Item description: The TTL used when re-creating IPv4 headers in ZOOM encoded packets received on this interface.
Type: Refer to - definitions->types->TTL
Default: 64

2.8.14.3 AssumedMTU

Property: Links :: ZOOM :: AssumedMTU
Item description: The assumed MTU of the ZOOM interface, used to reduce the space required for the IPv4 Total Length field. Used for both encoding and decoding. Auto-detected from ZOOM interface (or 1500 if unable to detect).
Type: Refer to - definitions->types->UINT16
Default: 1500

2.9 Plugins

Property: Plugins
Description: Array of plugin names to dynamically load to extend core functionality.
Type: Array of unique items.

Item type: Enum of , wlanmanager, vpn, flowredirector, freeboard, mantra, mre, radiocontroller, reconfiguration, visualizer, tscanr, bit, zoom, grekeepalive, zoomclient, sysconfig, find.
Default: None

2.10 AreshPort

Property: AreshPort
Description: The TCP port ARESH connects to in order to comminicate with ARES Core.
Type: Refer to - definitions->types->Port
Default: 12321

2.11 AllowRemoteAresh

Property: AllowRemoteAresh
Description: Flag indicating if ARES Core will accept connections not originating locally or not.
Type: Boolean true or false.
Default: False

2.12 FRR

Property: FRR
Description: Configuration for running FRR processes.
Type: JSON Object
Default: None

2.12.1 PreConfig

Property: FRR :: PreConfig
Description: FRR configuration that is applied before any additional ARES configuration. Commands are applied in order defined as if typed into the FRR shell.
Type: Array with a minimum number of 1 item(s).
Item type: String.
Default: None

2.12.2 PostConfig

Property: FRR :: PostConfig
Description: FRR configuration that is applied after initial ARES configuration is complete. Commands are applied in order defined as if typed into the FRR shell.
Type: Array with a minimum number of 1 item(s).
Item type: String.
Default: None

2.13 OSPF

Property: OSPF
Description: Global OSPF configuration of this router.
Type: JSON Object
Default: None

2.13.1 Area

Property: OSPF :: Area
Description: The global OSPF area used for all links/tunnels on this router.
Default: 0
Type: Refer to - definitions->ospf->OSPFArea
Default: None

2.13.2 AreaRanges

Property: OSPF :: AreaRanges
Description: Configuration of summerized network ranges advertised per OSPF area.
Type: Array of unique items and a minimum number of 1 item(s).
Item description: The network range advertized for the given OSPF area.
Item type: JSON Object
Required: ['Area', 'Range']
Default: None

2.13.2.1 Area

Property: OSPF :: AreaRanges :: Area
Item description: The OSPF area.
Type: Refer to - definitions->ospf->OSPFArea
Default: None

2.13.2.2 Range

Property: OSPF :: AreaRanges :: Range
Item description: The network range advertised in this OSPF area.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.13.3 AreaAuthentication

Property: OSPF :: AreaAuthentication
Description: Configuration of the OSPF per-area authentication.
Type: Array of unique items and a minimum number of 1 item(s).
Item description: Authentication type for the given OSPF area.
Item type: JSON Object
Required: ['Area', 'Type']
Default: None

2.13.3.1 Area
Property: OSPF :: AreaAuthentication :: Area
Item description: The OSPF area.
Type: Refer to - definitions->ospf->OSPFArea
Default: None

2.13.3.2 Type
Property: OSPF :: AreaAuthentication :: Type
Item description: Authentication type for this OSPF area.
Item type: String enum of password, digest.
Default: None

2.13.4 ABRType
Property: OSPF :: ABRType
Description: The ABR compatibility setting.
Type: Refer to - definitions->ospf->ABRTypes
Default: cisco

2.14 Multicast

Property: Multicast
Description: The global multicast configuration for the router.
Type: JSON Object
Required: ['Enabled']
Default: None

2.14.1 Enabled
Property: Multicast :: Enabled
Description: Enable/disable multicast globally for all links.
Type: Boolean true or false.
Default: False

2.14.2 IGMP
Property: Multicast :: IGMP
Description: Global IGMP configuration for all multicast enabled links.
Type: JSON Object
Default: None

2.14.2.1 Version
Property: Multicast :: IGMP :: Version
Description: The IGMP version to use on this link.
Type: Integer enum of 2, 3.
Default: 3

2.14.2.2 Query-Interval
Property: Multicast :: IGMP :: Query-Interval
Description: Time, in seconds, between sending IGMP General Query messages.
Type: Integer with a minimum of 1 and a maximum of 1800.
Default: 125

2.14.2.3 Query-Max-Response-Time
Property: Multicast :: IGMP :: Query-Max-Response-Time
Description: Maximum time, in deci-seconds, that a receiver has to respond to a query.
Type: Integer with a minimum of 10 and a maximum of 250.
Default: 10

2.14.2.4 Last-Member-Query-Count
Property: Multicast :: IGMP :: Last-Member-Query-Count
Description: Number of group queries to send when the last members leaves the group.
Type: Integer with a minimum of 1 and a maximum of 7.
Default: 2

2.14.2.5 Last-Member-Query-Interval
Property: Multicast :: IGMP :: Last-Member-Query-Interval
Description: Time, in deci-seconds, between sending last member queries.
Type: Integer with a minimum of 1 and a maximum of 255.
Default: 10

2.14.3 PIM
Property: Multicast :: PIM
Description: Global PIM configuration for all multicast enabled links.
Type: JSON Object
Default: None

2.14.3.1 RP-List
Property: Multicast :: PIM :: RP-List
Description: The list of RP routers for PIM-SM mode. Default to 127.0.0.1.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: JSON Object
Required: ['RP']
Default: None

2.14.3.1.1 RP
Property: Multicast :: PIM :: RP-List :: RP
Item description: The RP IPv4 address.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.14.3.1.2 Groups
Property: Multicast :: PIM :: RP-List :: Groups
Item description: One or more group prefix ranges handled by this RP. Must be provided if using more than one RP.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Or
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Default: None

2.14.3.2 RP-KeepAliveTimer
Property: Multicast :: PIM :: RP-KeepAliveTimer
Description: The time out value, in seconds, for a S,G flow to the RP.
Type: Integer with a minimum of 31 and a maximum of 60000.
Default: 210

2.14.3.3 SPT-Switchover
Property: Multicast :: PIM :: SPT-Switchover
Description: Enable/disable SPT switch-over by a last-hop router once multicast sources are learned.
Type: Boolean true or false.
Default: True

2.14.3.4 SPT-Groups
Property: Multicast :: PIM :: SPT-Groups
Description: Limit SPT switch-over to only these groups.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Default: None

2.14.3.5 ECMP
Property: Multicast :: PIM :: ECMP
Description: If PIM has a choice of ECMP nexthops for a particular RPF, PIM will cause S,G flows to be spread out amongst the nexthops. If this is disabled then the first nexthop found will be used.
Type: Boolean true or false.
Default: False

2.14.3.6 ECMP-Rebalance
Property: Multicast :: PIM :: ECMP-Rebalance
Description: If PIM is using ECMP and an interface goes down, cause PIM to rebalance all S,G flows across the remaining nexthops. If this is disabled then PIM only modifies those S,G flows that were using the interface that went down.
Type: Boolean true or false.

Default: False

2.14.3.7 Join-Prune-Interval
Property: Multicast :: PIM :: Join-Prune-Interval
Description: Time, in seconds, between sending Join-Prune messages.
Type: Integer with a minimum of 60 and a maximum of 600.
Default: 60

2.14.3.8 Keep-Alive-Timer
Property: Multicast :: PIM :: Keep-Alive-Timer
Description: Time, in seconds, that a multicast route is active, unless another Join is received.
Type: Integer with a minimum of 31 and a maximum of 60000.
Default: 210

2.14.3.9 Packets
Property: Multicast :: PIM :: Packets
Description: When processing packets from a neighbor process the given number of incoming packets at one time before moving on to the next task. The default value is 3 packets. This setting is only useful at scale when you can possibly have a large number of PIM control packets flowing.
Type: Integer with a minimum of 1 and a maximum of 100.
Default: 3

2.14.3.10 Register-Suppress-Time
Property: Multicast :: PIM :: Register-Suppress-Time
Description: Time, in seconds, that a DR stops sending Register-encapsulated data to the RP after receiving a Register-Stop.
Type: Integer with a minimum of 5 and a maximum of 60000.
Default: 60

2.14.3.11 Send-V6-Secondary
Property: Multicast :: PIM :: Send-V6-Secondary
Description: When sending PIM hello packets tell PIM to send any v6 secondary addresses on the interface. This information is used to allow PIM to use v6 nexthops in its decision for RPF lookup.
Type: Boolean true or false.
Default: False

2.14.3.12 SSM-Prefixlist
Property: Multicast :: PIM :: SSM-Prefixlist
Description: The list of multicast group prefix ranges that will be treated as SSM. Default: 232.0.0.0/8
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4MulticastMaskReq

Default: None

2.14.3.13 RPF-Lookup-Mode

Property: Multicast :: PIM :: RPF-Lookup-Mode
Description: Modify how PIM does RPF lookups in the zebra routing table. You can use these choices:
"longer-prefix"
Lookup the RPF in both tables using the longer prefix as a match
"lower-distance"
Lookup the RPF in both tables using the lower distance as a match
"mrib-only"
Lookup in the Multicast RIB only
"mrib-then-urib"
Lookup in the Multicast RIB then the Unicast Rib, returning first found.
"urib-only"
Lookup in the Unicast Rib only.
Type: String enum of longer-prefix, lower-distance, mrib-only, mrib-then-urib, urib-only.
Default: mrib-then-urib

2.14.3.14 BFD

Property: Multicast :: PIM :: BFD
Description: A detection protocol designed to provide fast forwarding path failure detection times. Interface specific, can be overridden by link configuration.
Type: Boolean true or false.
Default: False

2.14.3.15 BSM

Property: Multicast :: PIM :: BSM
Description: Allows an interface to process bootstrap messages. Interface specific, can be overridden by link configuration.
Type: Boolean true or false.
Default: True

2.14.3.16 Unicast-BSM

Property: Multicast :: PIM :: Unicast-BSM
Description: Allows an interface to process unicast bootstrap messages. Interface specific, can be overridden by link configuration.
Type: Boolean true or false.
Default: True

2.14.3.17 DR-Priority

Property: Multicast :: PIM :: DR-Priority
Description: The priority level used to influence DR election per-link. Interface specific, can be overridden by link configuration.

Type: Integer with a minimum of 1 and a maximum of 4294967295.
Default: 1

2.14.3.18 Hello-Interval

Property: Multicast :: PIM :: Hello-Interval
Description: The time, in seconds, between sending PIM hello messages. Interface specific, can be overridden by link configuration.
Type: Integer with a minimum of 1 and a maximum of 180.
Default: 30

2.14.3.19 Boundary-List

Property: Multicast :: PIM :: Boundary-List
Description: If a PIM join or IGMP report is received and the Group is defined here, PIM will ignore the join or report. Interface specific, can be overridden by link configuration.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Default: None

2.14.4 MRIB

Property: Multicast :: MRIB
Description: Routes used to influence Multicast RPF lookup. These routes are not installed nor used for normal rib processing and are only used for RPF lookup. It is possible to create weird states, use with caution.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: JSON Object
Required: ['Destination-Prefix', 'Next-Hop']
Default: None

2.14.4.1 Destination-Prefix

Property: Multicast :: MRIB :: Destination-Prefix
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.14.4.2 Next-Hop

Property: Multicast :: MRIB :: Next-Hop
Type: Refer to - definitions->types->IPv4Address
Or
Type: Refer to - definitions->types->InterfaceName
Default: None

2.14.4.3 Distance

Property: Multicast :: MRIB :: Distance
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.15 ControlDSCP

Property: ControlDSCP
Description: DSCP value set for control messages used by the internal routing protocols to ensure network integrity.
Type: Refer to - definitions->types->DSCP
Default: 1

2.16 PriorityDSCPValues

Property: PriorityDSCPValues
Description: The DSCP values used for traffic control that specify the priority levels. Array is ordered from highest priority to lowest.
Type: Array with a maximum number of 15 item(s) that must be unique.
Default: []
Type: Refer to - definitions->types->DSCP
Default: None

2.17 EdgeMode

Property: EdgeMode
Description: Run router in Edge mode when set.
Type: Boolean true or false.
Default: False

2.18 DesignatedRouter

Property: DesignatedRouter
Description: Configuration for this router in designated router election. If not configured, then this router will not be eligible for designated router.
Type: JSON Object
Required: ['Address']
Default: None

2.18.1 Address

Property: DesignatedRouter :: Address
Description: The address to be used for designated router election. Lowest designated address wins. This address must be unique in the network and not exist on any other links on this router. The designated address will be added to the designated interface (defaults to lo) and advertised as host route.
Type: Refer to - definitions->types->IPAddress
Default: None

2.18.2 Interface
Property: DesignatedRouter :: Interface
Description: The interface on which the designated address is added. Defaults to lo. It is recommended that this is not set to ensure proper reachability to the designated address.
Type: Refer to - definitions->types->InterfaceName
Default: lo

2.18.3 Advertise
Property: DesignatedRouter :: Advertise
Description: Flag indicating if the designated router address should be advertised to the network via OSPF or not. Designated router election will still happen if not advertised, but the designated router will not be reachable if it is not advertised so only disable this flag if you are sure it will be advertised via another protocol.
Type: Boolean true or false.
Default: True

2.19 NeighborDiscovery

Property: NeighborDiscovery
Description: Global configuration of the neighbor discovery process.
Type: JSON Object
Default: None

2.19.1 RequireSignature
Property: NeighborDiscovery :: RequireSignature
Description: Flag indicating whether or not to sign our discovery messages.
Type: Boolean true or false.
Default: True

2.19.2 UseCertificates
Property: NeighborDiscovery :: UseCertificates
Description: Use certificate exchange for signing instead of pre-shared keys.
Type: Boolean true or false.
Default: False

2.19.3 CertificatesPort
Property: NeighborDiscovery :: CertificatesPort
Description: The port used for transferring certificates.
Type: Refer to - definitions->types->Port
Default: 12344

2.20 Quarantined

Property: Quarantined

Description: List of router ID's that need to be quarantined from the network.
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->UINT32
Or
Type: Refer to - definitions->types->DottedQuad
Default: None

2.21 UseThrowableGRE

Property: UseThrowableGRE
Description: Uses throwable addresses for GRE tunnels when set. Randomly picked within the 10.250.x.x-10.254.x.x range.
Type: Boolean true or false.
Default: False

2.22 KeepGRERoutes

Property: KeepGRERoutes
Description: Keep the default routes that the kernel sets up when the GRE tunnel is created, when set.
Type: Boolean true or false.
Default: False

2.23 CutThruRouting

Property: CutThruRouting
Description: Uses cut-thru routing when set.
Type: Boolean true or false.
Default: True

2.24 NeighborPolicyRouting

Property: NeighborPolicyRouting
Description: Enables policy routing to allow ARES to direct traffic flows through specific neighbors.
Type: Boolean true or false.
Default: False

2.25 Mobility

Property: Mobility
Description: Configuration of Mobility parameters for a mobile router.
Type: JSON Object
Required: ['PortableAddress', 'PortableSubnets']

Default: None

2.25.1 PortableAddress
Property: Mobility :: PortableAddress
Description: The Portable address of this router, if required.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

PortableSubnets

2.25.2 Property: Mobility :: PortableSubnets
Description: The subnet ranges designated for Portable addresses so that they can be detected and routed correctly.
Type: Array of unique items.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.25.3 ServicePort
Property: Mobility :: ServicePort
Description: The port used when sending requests to the mobility server.
Type: Refer to - definitions->types->Port
Default: 12346

2.25.4 ResponsePort
Property: Mobility :: ResponsePort
Description: The port used when getting responses from the mobility server.
Type: Refer to - definitions->types->Port
Default: 12347

2.25.5 RegistrationInterval
Property: Mobility :: RegistrationInterval
Description: The time, in seconds, between registering mobility addresses to the mobility server.
Type: Integer with a minimum of 5 and a maximum of 600.
Default: 30

2.25.6 RegistrationTimeout
Property: Mobility :: RegistrationTimeout
Description: The time, in seconds, before the mobility server times out a portable address registration.
Type: Integer with a minimum of 5 and a maximum of 600.
Default: 120

2.25.7 TranslationTimeout
Property: Mobility :: TranslationTimeout

Description: The time, in seconds, before the mobility client refreshes the mobility translation from the mobility server.
Type: Integer with a minimum of 5 and a maximum of 600.
Default: 30

2.25.8 UsageTimeout
Property: Mobility :: UsageTimeout
Description: The time, in minutes, before the mobility client stops keeping an address translation up to date.
Type: Integer with a minimum of 1 and a maximum of 10.
Default: 5

2.26 VPN

Property: VPN
Description: The configuration of a security profile which follows NIAP Security Guidelines.
Type: JSON Object
Default: None

2.26.1 Modules
Property: VPN :: Modules
Description: Configuration parameters from strongswan.conf
Type: JSON Object
Default: None

2.26.1.1 charon-systemd
Property: VPN :: Modules :: charon-systemd
Description: Options applying to the charon-systemd daemon
Type: JSON Object
Default: None

2.26.1.1.1 accept_private_algs
Property: VPN :: Modules :: charon-systemd :: accept_private_algs
Description: Deliberately violate the IKE standard's requirement and allow the use of private algorithm identifiers, even if the peer implementation is unknown (i.e. if the peer doesn't send a vendor ID via send_vendor_id)
Type: Boolean true or false.
Default: False

2.26.1.1.2 block_threshold
Property: VPN :: Modules :: charon-systemd :: block_threshold
Description: Maximum number of half-open IKE_SAs (including unprocessed IKE_SA_INITs) for a single peer IP
Type: Integer with a minimum of 0.

Default: 5

2.26.1.1.3 cache_crls
Property: VPN :: Modules :: charon-systemd :: cache_crls
Description: Whether Certicate Revocation Lists (CRLs) fetched via HTTP or LDAP should be saved under a unique file name derived from the public key of the Certification Authority (CA) to the x509crl directory
Type: Boolean true or false.
Default: False

2.26.1.1.4 check_current_path
Property: VPN :: Modules :: charon-systemd :: check_current_path
Description: By default, after detecting any changes to interfaces and/or addresses no action is taken if the current path to the remote peer still looks usable. Enabling this option will use DPD to check if the path actually still works, or, for instance, the peer removed the state after a longer phase without connectivity. It will also trigger a MOBIKE update if NAT mappings were removed during the downtime
Type: Boolean true or false.
Default: False

2.26.1.1.5 cert_cache
Property: VPN :: Modules :: charon-systemd :: cert_cache
Description: Whether relations in validated certificate chains should be cached in memory
Type: Boolean true or false.
Default: True

2.26.1.1.6 cisco_flexvpn
Property: VPN :: Modules :: charon-systemd :: cisco_flexvpn
Description: Send the Cisco FlexVPN vendor ID payload (IKEv2 only), which is required in order to make Cisco brand devices allow negotiating a local traffic selector (from strongSwan's point of view) that is not the assigned virtual IP address if such an address is requested by strongSwan. Sending the Cisco FlexVPN vendor ID prevents the peer from narrowing the initiator's local traffic selector and allows it to e.g. negotiate a TS of 0.0.0.0/0 == 0.0.0.0/0 instead. This has been tested with a "tunnel mode ipsec ipv4" Cisco template but should also work for GRE encapsulation
Type: Boolean true or false.
Default: False

2.26.1.1.7 cisco_unity
Property: VPN :: Modules :: charon-systemd :: cisco_unity
Description: Send Cisco Unity vendor ID payload (IKEv1 only), see unity plugin
Type: Boolean true or false.
Default: False

2.26.1.1.8 close_ike_on_child_failure
Property: VPN :: Modules :: charon-systemd :: close_ike_on_child_failure
Description: Close the IKE SA if setup of the CHILD SA along with IKE_AUTH failed
Type: Boolean true or false.
Default: False

2.26.1.1.9 cookie_threshold
Property: VPN :: Modules :: charon-systemd :: cookie_threshold
Description: Number of half-open IKE_SAs (including unprocessed IKE_SA_INITs) that activate the cookie mechanism
Type: Integer with a minimum of 0.
Default: 30

2.26.1.1.10 cookie_threshold_ip
Property: VPN :: Modules :: charon-systemd :: cookie_threshold_ip
Description: Number of half-open IKE_SAs (including unprocessed IKE_SA_INITs) for a single peer IP that activate the cookie mechanism (since version 5.9.6)
Type: Integer with a minimum of 0.
Default: 3

2.26.1.1.11 crypto_test
Property: VPN :: Modules :: charon-systemd :: crypto_test
Description: Section to configure crypto tests
Type: JSON Object
Default: None

2.26.1.1.11.1 bench
Property: VPN :: Modules :: charon-systemd :: crypto_test :: bench
Description: Benchmark crypto algorithms and order them by efficiency
Type: Boolean true or false.
Default: False

2.26.1.1.11.2 bench_size
Property: VPN :: Modules :: charon-systemd :: crypto_test :: bench_size
Description: Buffer size used for crypto benchmark
Type: Integer with a minimum of 0.
Default: 1024

2.26.1.1.11.3 bench_time
Property: VPN :: Modules :: charon-systemd :: crypto_test :: bench_time
Description: Time in ms during which crypto algorithm performance is measured
Type: Integer with a minimum of 0.
Default: 50

2.26.1.1.11.4 on_add

Property: VPN :: Modules :: charon-systemd :: crypto_test :: on_add
Description: Test crypto algorithms during registration (requires test vectors provided by the test-vectors plugin)
Type: Boolean true or false.
Default: False

2.26.1.1.11.5 on_create
Property: VPN :: Modules :: charon-systemd :: crypto_test :: on_create
Description: Test crypto algorithms on each crypto primitive instantiation
Type: Boolean true or false.
Default: False
Required: {'description': 'Strictly require at least one test vector to enable an algorithm', 'type': 'boolean', 'default': False}
Default: None

2.26.1.1.11.6 rng_true
Property: VPN :: Modules :: charon-systemd :: crypto_test :: rng_true
Description: Whether to test RNG with TRUE quality. Requires a lot of entropy
Type: Boolean true or false.
Default: False

2.26.1.1.12 delete_rekeyed
Property: VPN :: Modules :: charon-systemd :: delete_rekeyed
Description: Delete CHILD_SAs right after they got successfully rekeyed (IKEv1 only). Reduces the number of stale CHILD_SAs in scenarios with a lot of rekeyings. However this might cause problems with implementations that continue to use rekeyed SAs until they expire
Type: Boolean true or false.
Default: False

2.26.1.1.13 delete_rekeyed_delay
Property: VPN :: Modules :: charon-systemd :: delete_rekeyed_delay
Description: Delay in seconds until inbound IPsec SAs are deleted after rekeyings (IKEv2 only). To process delayed packets the inbound part of a CHILD_SA is kept installed up to the configured number of seconds after it got replaced during a rekeying. If set to 0 the CHILD_SA will be kept installed until it expires. If no lifetime is set it will be destroyed immediately
Type: Integer with a minimum of 0.
Default: 5

2.26.1.1.14 dh_exponent_ansi_x9_42
Property: VPN :: Modules :: charon-systemd :: dh_exponent_ansi_x9_42
Description: Use ANSI X9.42 DH exponent size or optimum size matched to cryptographical strength
Type: Boolean true or false.
Default: True

2.26.1.1.15 dlopen_use_rtld_now
Property: VPN :: Modules :: charon-systemd :: dlopen_use_rtld_now
Description: Use RTLD_NOW with dlopen() when loading plugins to reveal missing symbols immediately.
Type: Boolean true or false.
Default: False

2.26.1.1.16 dns1
Property: VPN :: Modules :: charon-systemd :: dns1
Description: DNS server assigned to peer via configuration payload (CP), see attr plugin
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.1.1.17 dns2
Property: VPN :: Modules :: charon-systemd :: dns2
Description: DNS server assigned to peer via configuration payload (CP), see attr plugin
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.1.1.18 dos_protection
Property: VPN :: Modules :: charon-systemd :: dos_protection
Description: Enable Denial of Service protection using cookies and aggressiveness checks
Type: Boolean true or false.
Default: True

2.26.1.1.19 filelog
Property: VPN :: Modules :: charon-systemd :: filelog
Description: Section to define file loggers
Type: JSON Object
Default: None

2.26.1.1.19.1 filelog :: <pattern>
Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$
Description: An arbitrarily-named logger section
Type: JSON Object
Required: ['path']
Default: None

2.26.1.1.19.1.1 ^[a-zA-Z0-9_-]+$ :: <pattern>

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: ^(app|asn|cfg|chd|dmn|enc|esp|ike|job|knl|lib|mgr|net|tls)$
Description: Log level for a specific subsystem
app - applications other than daemons
asn - Low-level encoding/decoding (ASN.1, X.509 etc.)

cfg - Configuration management and plugins
chd - CHILD_SA/IPsec SA
dmn - Main daemon setup/cleanup/signal handling
enc - Packet encoding/decoding encryption/decryption operations
esp - libipsec library messages
ike - IKE_SA/ISAKMP SA
job - Jobs queuing/processing and thread pool management
knl - IPsec/Networking kernel interface
lib - libstrongswan library messages
mgr - IKE_SA manager, handling synchronization for IKE_SA access
net - IKE network communication
tls - libtls library messages
Type: Integer enum of -1, 0, 1, 2, 3, 4.
Default: 1

2.26.1.1.19.1.2path

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: path
Description: The name of the log file (ending in .log) or stderr/stdout
Type: String enum of stdout, stderr.
Or
Type: String pattern of ^[a-zA-Z0-9_ \.\-]{1,}\.log$.
Default: {'description': 'Specifies the default loglevel to be used for subsystems for which no specific loglevel is defined\n-1: Absolutely silent\n0: Very basic auditing logs, (e.g. SA up/SA down)\n1: Generic control flow with errors, a good default to see whats going on\n2: More detailed debugging control flow\n3: Including RAW data dumps in hex\n4: Also include sensitive material in dumps, e.g. keys', 'type': 'integer', 'enum': [-1, 0, 1, 2, 3, 4], 'default': 1}

2.26.1.1.19.1.3append

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: append
Description: If this option is enabled log entries are appended to the existing file
Type: Boolean true or false.
Default: True

2.26.1.1.19.1.4flush_line

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: flush_line
Description: Enabling this option disables block buffering and enables line buffering, i.e. a flush to disk is enforced for each logged line
Type: Boolean true or false.
Default: False

2.26.1.1.19.1.5ike_name

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: ike_name
Description: Prefix each log entry with the connection name and a unique numerical identifier for each IKE_SA

Type: Boolean true or false.
Default: False

2.26.1.1.19.1.6log_level

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: log_level
Description: Add the log level of each message after the subsystem
Type: Boolean true or false.
Default: False

2.26.1.1.19.1.7time_format

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: time_format
Description: Prefix each log entry with a timestamp. The option accepts a format string as passed to strftime(3)
Type: String.
Default: %Y-%m-%d %H:%M:%S

2.26.1.1.19.1.8time_add_ms

Property: VPN :: Modules :: charon-systemd :: filelog :: ^[a-zA-Z0-9_-]+$ :: time_add_ms
Description: Adds the milliseconds within the current second after the timestamp (separated by a dot so time_format should end with %S or %T)
Type: Boolean true or false.
Default: False

2.26.1.1.20 flush_auth_cfg
Property: VPN :: Modules :: charon-systemd :: flush_auth_cfg
Description: If enabled objects used during authentication (certificates, identities etc.) are released to free memory once an IKE_SA is established. Enabling this might conflict with plugins that later need access to e.g. the used certificates
Type: Boolean true or false.
Default: False

2.26.1.1.21 follow_redirects
Property: VPN :: Modules :: charon-systemd :: follow_redirects
Description: Whether to follow IKEv2 redirects, see RFC 5685
Type: Boolean true or false.
Default: True

2.26.1.1.22 force_eap_only_authentication
Property: VPN :: Modules :: charon-systemd :: force_eap_only_authentication
Description: Violate the EAP-only authentication requirements according to RFC 5998, even if the peer did not send an EAP_ONLY_AUTHENTICATION notify during IKE_AUTH
Type: Boolean true or false.
Default: False

2.26.1.1.23 fragment_size

Property: VPN :: Modules :: charon-systemd :: fragment_size
Description: Maximum size (complete IP datagram size in bytes) of a sent IKE fragment when using proprietary IKEv1 or standardized IKEv2 fragmentation. If specified, this limit is used for both IPv4 and IPv6 with a default of 1280 bytes. Use 0 for the address-family-specific default values defined by RFC 7383 which specifies a very conservative limit of 576 bytes for IPv4 but sets the limit to 1280 bytes for IPv6.
Type: Integer with a minimum of 0.
Default: 1280

2.26.1.1.24 group

Property: VPN :: Modules :: charon-systemd :: group
Description: Name of the group the daemon changes to after startup
Type: String.
Default: None

2.26.1.1.25 half_open_timeout

Property: VPN :: Modules :: charon-systemd :: half_open_timeout
Description: Timeout in seconds for connecting IKE_SAs
Type: Integer with a minimum of 0.
Default: 30

2.26.1.1.26 hash_and_url

Property: VPN :: Modules :: charon-systemd :: hash_and_url
Description: Enable hash and URL support
Type: Boolean true or false.
Default: False

2.26.1.1.27 host_resolver

Property: VPN :: Modules :: charon-systemd :: host_resolver
Type: JSON Object
Default: None

2.26.1.1.27.1 max_threads

Property: VPN :: Modules :: charon-systemd :: host_resolver :: max_threads
Description: Maximum number of concurrent resolver threads (they are terminated if unused)
Type: Integer with a minimum of 1.
Default: 3

2.26.1.1.27.2 min_threads

Property: VPN :: Modules :: charon-systemd :: host_resolver :: min_threads
Description: Minimum number of resolver threads to keep around
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.28 ignore_acquire_ts

Property: VPN :: Modules :: charon-systemd :: ignore_acquire_ts
Description: If this is disabled the traffic selectors from the kernel's acquire events, which are derived from the triggering packet, are prepended to the traffic selectors from the configuration for IKEv2 connection. By enabling this, such specific traffic selectors will be ignored and only the ones in the config will be sent. This always happens for IKEv1 connections as the protocol only supports one set of traffic selectors per CHILD SA
Type: Boolean true or false.
Default: False

2.26.1.1.29 ignore_routing_tables

Property: VPN :: Modules :: charon-systemd :: ignore_routing_tables
Description: A list of routing tables to be excluded from route lookup
Type: Array with a minimum number of 1 item(s).
Item type: String.
Default: None

2.26.1.1.30 ikesa_limit

Property: VPN :: Modules :: charon-systemd :: ikesa_limit
Description: Maximum number of IKE_SAs that can be established at the same time before new connection attempts are blocked
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.31 ikesa_table_segments

Property: VPN :: Modules :: charon-systemd :: ikesa_table_segments
Description: Number of exclusively locked segments in the hash table. The number of segments is at least one, at most the size of the hash table, and should be a power of two. Using more than 512 segments may lead to instabilities on some systems.
Type: Integer with a minimum of 1.
Default: 1

2.26.1.1.32 ikesa_table_size

Property: VPN :: Modules :: charon-systemd :: ikesa_table_size
Description: Size of the IKE SA hash table. Must be a power of two. 5 to 20 IKE_SAs in each hash table entry is probably a good value (e.g. hash table size of 1,000 to 4,000 for 20,000 expected clients)
Type: Integer with a minimum of 1.
Default: 1

2.26.1.1.33 inactivity_close_ike

Property: VPN :: Modules :: charon-systemd :: inactivity_close_ike
Description: Whether to close IKE_SA if the only CHILD SA closed due to inactivity

Type: Boolean true or false.
Default: False

2.26.1.1.34 init_limit_half_open

Property: VPN :: Modules :: charon-systemd :: init_limit_half_open
Description: Limit new connections based on the current number of half open IKE_SAs (in connecting state but not yet established). If your responder is capable of negotiating 100 tunnels/s, you might set this limit to 1000.
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.35 init_limit_job_load

Property: VPN :: Modules :: charon-systemd :: init_limit_job_load
Description: Limit new connections based on the number of jobs currently queued for processing. Includes load from other jobs such as rekeying. Choosing a good value is difficult, do not set unless you understand what you're doing.
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.36 initiator_only

Property: VPN :: Modules :: charon-systemd :: initiator_only
Description: Causes charon daemon to ignore IKE initiation requests
Type: Boolean true or false.
Default: False

2.26.1.1.37 install_routes

Property: VPN :: Modules :: charon-systemd :: install_routes
Description: Install routes into a separate routing table for established IPsec tunnels. If disabled a more efficient lookup for source and next-hop addresses is used.
Type: Boolean true or false.
Default: True

2.26.1.1.38 install_virtual_ip

Property: VPN :: Modules :: charon-systemd :: install_virtual_ip
Description: Install virtual IP addresses
Type: Boolean true or false.
Default: True

2.26.1.1.39 install_virtual_ip_on

Property: VPN :: Modules :: charon-systemd :: install_virtual_ip_on
Description: The name of the interface on which virtual IP addresses should be installed. If not specified the addresses will be installed on the outbound interface
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.40 integrity_test

Property: VPN :: Modules :: charon-systemd :: integrity_test
Description: Check charon daemon, libcharon, libstrongswan and other strongSwan libraries as well as plugin integrity at startup
Type: Boolean true or false.
Default: False

2.26.1.1.41 interfaces_ignore

Property: VPN :: Modules :: charon-systemd :: interfaces_ignore
Description: A list of network interfaces that should be ignored by the charon daemon. If interfaces_use is specified, this option has no effect
Type: Array.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.42 interfaces_use

Property: VPN :: Modules :: charon-systemd :: interfaces_use
Description: A list of network interfaces that should be used by the charon daemon. All other interfaces are ignored
Type: Array.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.43 journal

Property: VPN :: Modules :: charon-systemd :: journal
Description: Section to configure native systemd journal logger, very similar to the syslog logger.
Type: JSON Object
Default: {'description': 'Specifies the default loglevel to be used for subsystems for which no specific loglevel is defined\n-1: Absolutely silent\n0: Very basic auditing logs, (e.g. SA up/SA down)\n1: Generic control flow with errors, a good default to see whats going on\n2: More detailed debugging control flow\n3: Including RAW data dumps in hex\n4: Also include sensitive material in dumps, e.g. keys', 'type': 'integer', 'enum': [-1, 0, 1, 2, 3, 4], 'default': 1}

2.26.1.1.43.1 journal :: <pattern>

Property: VPN :: Modules :: charon-systemd :: journal ::
^(app|asn|cfg|chd|dmn|enc|esp|ike|job|knl|lib|mgr|net|tls)$
Description: Log level for a specific subsystem
app - applications other than daemons
asn - Low-level encoding/decoding (ASN.1, X.509 etc.)
cfg - Configuration management and plugins
chd - CHILD_SA/IPsec SA
dmn - Main daemon setup/cleanup/signal handling

enc - Packet encoding/decoding encryption/decryption operations
esp - libipsec library messages
ike - IKE_SA/ISAKMP SA
job - Jobs queuing/processing and thread pool management
knl - IPsec/Networking kernel interface
lib - libstrongswan library messages
mgr - IKE_SA manager, handling synchronization for IKE_SA access
net - IKE network communication
tls - libtls library messages
Type: Integer enum of -1, 0, 1, 2, 3, 4.
Default: 1

2.26.1.1.44 keep_alive

Property: VPN :: Modules :: charon-systemd :: keep_alive
Description: NAT keep alive interval in seconds
Type: Integer with a minimum of 0.
Default: 20

2.26.1.1.45 keep_alive_dpd_margin

Property: VPN :: Modules :: charon-systemd :: keep_alive_dpd_margin
Description: Number of seconds the keep alive interval may be exceeded before a DPD is sent instead of a NAT keep alive (0 to disable). This is only useful if a clock is used that includes time spent suspended (e.g. CLOCK_BOOTTIME)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.46 leak_detective

Property: VPN :: Modules :: charon-systemd :: leak_detective
Description: Section to configure the internal memory leak detective
Type: JSON Object
Default: None

2.26.1.1.46.1 detailed

Property: VPN :: Modules :: charon-systemd :: leak_detective :: detailed
Description: Includes source file names and line numbers in leak detective output
Type: Boolean true or false.
Default: True

2.26.1.1.46.2 usage_threshold

Property: VPN :: Modules :: charon-systemd :: leak_detective :: usage_threshold
Description: Threshold in bytes for allocations to be included in usage reports (0 to include all). [10240]
Type: Integer with a minimum of 0.
Default: 10240

2.26.1.1.46.3 usage_threshold_count

Property: VPN :: Modules :: charon-systemd :: leak_detective :: usage_threshold_count
Description: Threshold in number of allocations for allocations to be included in usage reports (0 to include all)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.47 load_modular

Property: VPN :: Modules :: charon-systemd :: load_modular
Description: If enabled, the list of plugins to load is determined by individual load settings for each plugin (only those plugins explicitly setting load = true are loaded). If not enabled, all plugins are loaded unless their load properties are set to false.
Type: Boolean true or false.
Default: False

2.26.1.1.48 make_before_break

Property: VPN :: Modules :: charon-systemd :: make_before_break
Description: Initiate IKEv2 reauthentication with a make-before-break instead of a break-before-make scheme. Make-before-break uses overlapping IKE and CHILD SA during reauthentication by first recreating all new SAs before deleting the old ones. This behavior can be beneficial to avoid connectivity gaps during reauthentication, but requires support for overlapping SAs by the peer.
Type: Boolean true or false.
Default: True

2.26.1.1.49 max_ikev1_exchanges

Property: VPN :: Modules :: charon-systemd :: max_ikev1_exchanges
Description: Maximum number of IKEv1 phase 2 exchanges per IKE_SA to keep state about and track concurrently
Type: Integer with a minimum of 1.
Default: 3

2.26.1.1.50 max_packet

Property: VPN :: Modules :: charon-systemd :: max_packet
Description: Maximum packet size in bytes accepted by charon
Type: Integer with a minimum of 0.
Default: 10000

2.26.1.1.51 multiple_authentication

Property: VPN :: Modules :: charon-systemd :: multiple_authentication
Description: Enable multiple authentication exchanges, see RFC 4739
Type: Boolean true or false.
Default: True

2.26.1.1.52 nbns1
Property: VPN :: Modules :: charon-systemd :: nbns1
Description: WINS server assigned to peer via configuration payload (CP), see attr plugin
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.1.1.53 nbns2
Property: VPN :: Modules :: charon-systemd :: nbns2
Description: WINS server assigned to peer via configuration payload (CP), see attr plugin
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.1.1.54 ocsp_nonce_len
Property: VPN :: Modules :: charon-systemd :: ocsp_nonce_len
Description: Length of nonces in OCSP requests. According to RFC 8954, valid values are between 1 and 32, with new clients required to use 32. Some servers might not support that so lowering the value to e.g. 16 might be necessary.
Type: Integer with a minimum of 1 and a maximum of 32.
Default: 32

2.26.1.1.55 port
Property: VPN :: Modules :: charon-systemd :: port
Description: UDP port used locally. If set to 0 a random port will be allocated
Type: Integer with a minimum of 0 and a maximum of 49151.
Default: 500

2.26.1.1.56 port_nat_t
Property: VPN :: Modules :: charon-systemd :: port_nat_t
Description: UDP port used locally in case of NAT-T. If set to 0 a random port will be allocated. Has to be different from port, otherwise a random port will be allocated
Default: 4500

2.26.1.1.57 prefer_best_path
Property: VPN :: Modules :: charon-systemd :: prefer_best_path
Description: By default, charon keeps SAs on the routing path with addresses it previously used if that path is still usable. By enabling this option, it tries more aggressively to update SAs with MOBIKE on routing priority changes using the cheapest path. This adds more noise, but allows to dynamically adapt SAs to routing priority changes. This option has no effect if MOBIKE is not supported or disabled
Type: Boolean true or false.
Default: False

2.26.1.1.58 prefer_configured_proposals
Property: VPN :: Modules :: charon-systemd :: prefer_configured_proposals

Description: Prefer locally configured proposals for IKE/IPsec over supplied ones as responder (disabling this can avoid keying retries due to INVALID_KE_PAYLOAD notifies)
Type: Boolean true or false.
Default: True

2.26.1.1.59 prefer_temporary_addrs

Property: VPN :: Modules :: charon-systemd :: prefer_temporary_addrs
Description: By default public IPv6 addresses are preferred over temporary ones according to RFC 4941 to make connections more stable. Enable this option to reverse this.
Type: Boolean true or false.
Default: False

2.26.1.1.60 process_route

Property: VPN :: Modules :: charon-systemd :: process_route
Description: Process RTM_NEWROUTE and RTM_DELROUTE events
Type: Boolean true or false.
Default: True

2.26.1.1.61 processor

Property: VPN :: Modules :: charon-systemd :: processor
Description: Section to configure processor options
Type: JSON Object
Default: None

2.26.1.1.61.1 priority_threads

Property: VPN :: Modules :: charon-systemd :: processor :: priority_threads
Description: Subsection to configure the number of reserved threads per priority class
Type: JSON Object
Default: None

2.26.1.1.61.1.1 critical

Property: VPN :: Modules :: charon-systemd :: processor :: priority_threads :: critical
Description: Threads reserved for CRITICAL priority class jobs. It is usually not required to reserve threads for CRITICAL jobs as they rarely return.
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.61.1.2 high

Property: VPN :: Modules :: charon-systemd :: processor :: priority_threads :: high
Description: Threads reserved for HIGH priority class jobs. One or two should be sufficient.
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.61.1.3 medium

Property: VPN :: Modules :: charon-systemd :: processor :: priority_threads :: medium
Description: Threads reserved for MEDIUM priority class jobs. Threads for 1-2x the number of CPU cores should be enough.
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.61.1.4low

Property: VPN :: Modules :: charon-systemd :: processor :: priority_threads :: low
Description: Threads reserved for LOW priority class jobs. Reserving threads for LOW priority jobs does not currently make sense as all remaining threads are available.
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.62 rdn_matching
Property: VPN :: Modules :: charon-systemd :: rdn_matching
Description: How the Relative Distinguished Names (RDNs) a certificate's Subject Distinguished Name (DN) is composed of, are matched against configured identities. Possible values are strict (the default), reordered, and relaxed. With strict the number, type and order of all RDNs have to match. Wildcards (*) for RDN values are allowed (that's the case for all three variants). Using reordered also matches a DN if the RDNs appear in a different order, The number and type still have to match. Finally relaxed also allows matches of DNs that contain more RDNs than the configured identity (missing RDNs are treated like a wildcard match). Note that reordered and relaxed impose a considerable overhead on memory usage and runtime, in particular for mismatches as compared to strict.
Type: String enum of strict, reordered, relaxed.
Default: strict

2.26.1.1.63 receive_delay
Property: VPN :: Modules :: charon-systemd :: receive_delay
Description: Delay in ms for receiving packets, to simulate a larger Round Trip Time (RTT)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.64 receive_delay_response
Property: VPN :: Modules :: charon-systemd :: receive_delay_response
Description: Delay response messages
Type: Boolean true or false.
Default: True

2.26.1.1.65 receive_delay_request
Property: VPN :: Modules :: charon-systemd :: receive_delay_request
Description: Delay request messages
Type: Boolean true or false.
Default: True

2.26.1.1.66 receive_delay_type

Property: VPN :: Modules :: charon-systemd :: receive_delay_type
Description: Specific IKEv2 message type to delay, 0 for any (see IKEv2 Exchange Types)
Type: Refer to - definitions->types->UINT8
Default: 0

2.26.1.1.67 replay_window

Property: VPN :: Modules :: charon-systemd :: replay_window
Description: Size of the AH/ESP replay window, in packets
Type: Integer with a minimum of 0.
Default: 32

2.26.1.1.68 reqid_base

Property: VPN :: Modules :: charon-systemd :: reqid_base
Description: Value of the first reqid to be automatically assigned to a CHILD_SA
Type: Refer to - definitions->types->UINT32
Default: 1

2.26.1.1.69 retransmit_base

Property: VPN :: Modules :: charon-systemd :: retransmit_base
Description: Base to use for calculating exponential back off
Type: Number.
Default: 1.8

2.26.1.1.70 retransmit_jitter

Property: VPN :: Modules :: charon-systemd :: retransmit_jitter
Description: Maximum jitter in percent to apply randomly to calculated retransmission timeout (0 to disable)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.71 retransmit_limit

Property: VPN :: Modules :: charon-systemd :: retransmit_limit
Description: Upper limit in seconds for calculated retransmission timeout (0 to disable)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.72 retransmit_timeout

Property: VPN :: Modules :: charon-systemd :: retransmit_timeout
Description: Timeout in seconds before sending first retransmit
Type: Number.
Default: 4.0

2.26.1.1.73 retransmit_tries

Property: VPN :: Modules :: charon-systemd :: retransmit_tries
Description: Number of times to retransmit a packet before giving up
Type: Integer with a minimum of 0.
Default: 5

2.26.1.1.74 retry_initiate_interval

Property: VPN :: Modules :: charon-systemd :: retry_initiate_interval
Description: Interval in seconds to use when retrying to initiate an IKE SA e.g. if DNS resolution failed (0 to disable retries)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.75 reuse_ikesa

Property: VPN :: Modules :: charon-systemd :: reuse_ikesa
Description: Initiate CHILD_SA within existing IKE_SAs (always enabled for IKEv1)
Type: Boolean true or false.
Default: True

2.26.1.1.76 routing_table

Property: VPN :: Modules :: charon-systemd :: routing_table
Description: Numerical routing table to install routes to
Type: Refer to - definitions->types->UINT32
Default: 220

2.26.1.1.77 routing_table_prio

Property: VPN :: Modules :: charon-systemd :: routing_table_prio
Description: Priority of the routing table
Type: Refer to - definitions->types->UINT32
Default: 220

2.26.1.1.78 rsa_pss

Property: VPN :: Modules :: charon-systemd :: rsa_pss
Description: Whether to use RSA with PSS padding instead of PKCS#1 padding by default
Type: Boolean true or false.
Default: True

2.26.1.1.79 rsa_pss_trailerfield

Property: VPN :: Modules :: charon-systemd :: rsa_pss_trailerfield
Description: Whether to encode an explicit trailerField value of 0x01 in the RSA-PSS algorithmIdentifier (as documented in RFC 7427) or using the DEFAULT value by omitting the trailerField

Type: Boolean true or false.
Default: False

2.26.1.1.80 send_delay

Property: VPN :: Modules :: charon-systemd :: send_delay
Description: Delay in ms for sending packets, to simulate a larger Round Trip Time (RTT)
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.81 send_delay_request

Property: VPN :: Modules :: charon-systemd :: send_delay_request
Description: Delay request messages
Type: Boolean true or false.
Default: True

2.26.1.1.82 send_delay_response

Property: VPN :: Modules :: charon-systemd :: send_delay_response
Description: Delay response messages
Type: Boolean true or false.
Default: True

2.26.1.1.83 send_delay_type

Property: VPN :: Modules :: charon-systemd :: send_delay_type
Description: Specific IKEv2 message type to delay (0 for any) (see IKEv2 Exchange Types)
Type: Refer to - definitions->types->UINT8
Default: 0

2.26.1.1.84 send_vendor_id

Property: VPN :: Modules :: charon-systemd :: send_vendor_id
Description: Send strongSwan vendor ID payload
Type: Boolean true or false.
Default: False

2.26.1.1.85 signature_authentication

Property: VPN :: Modules :: charon-systemd :: signature_authentication
Description: Whether to enable Signature Authentication as per RFC 7427
Type: Boolean true or false.
Default: True

2.26.1.1.86 signature_authentication_constraints

Property: VPN :: Modules :: charon-systemd :: signature_authentication_constraints

Description: If enabled, signature schemes configured in remote.auth, in addition to getting used as constraints against signature schemes employed in the certificate chain, are also used as constraints against the signature scheme used by peers during IKEv2
Type: Boolean true or false.
Default: True

2.26.1.1.87 spi_label
Property: VPN :: Modules :: charon-systemd :: spi_label
Description: Value mixed into the local IKE SPIs after applying spi_mask
Type: String.
Default: 0x0000000000000000

2.26.1.1.88 spi_mask
Property: VPN :: Modules :: charon-systemd :: spi_mask
Description: Mask applied to local IKE SPIs before mixing in spi_label (bits set will be replaced with spi_label)
Type: String.
Default: 0x0000000000000000

2.26.1.1.89 spi_min
Property: VPN :: Modules :: charon-systemd :: spi_min
Description: The lower limit for SPIs requested from the kernel for IPsec SAs. Should not be set lower than 0x00000100 (256) as SPIs between 1 and 255 are reserved by IANA
Type: String.
Default: 0xc0000000

2.26.1.1.90 spi_max
Property: VPN :: Modules :: charon-systemd :: spi_max
Description: The upper limit for SPIs requested from the kernel for IPsec SAs
Type: String.
Default: 0xcfffffff

2.26.1.1.91 start-scripts
Property: VPN :: Modules :: charon-systemd :: start-scripts
Description: Section containing a list of scripts (name = path) that are executed when the daemon is started
Type: Array.
Item type: String.
Default: None

2.26.1.1.92 stop-scripts
Property: VPN :: Modules :: charon-systemd :: stop-scripts
Description: Section containing a list of scripts (name = path) that are executed when the daemon is terminated

Type: Array.
Item type: String.
Default: None

2.26.1.1.93 syslog
Property: VPN :: Modules :: charon-systemd :: syslog
Description: Section to define syslog loggers
Type: JSON Object
Default: None

2.26.1.1.93.1 identifier
Property: VPN :: Modules :: charon-systemd :: syslog :: identifier
Description: Global identifier used for an openlog(3) call prepended to each log message by syslog. If not configured, openlog(3) is not called. Thus the value will depend on system defaults (often the program name)
Type: String.
Default: None

2.26.1.1.93.2 syslog :: <pattern>
Property: VPN :: Modules :: charon-systemd :: syslog :: ^(auth|daemon)$
Description: The facility to set syslog options for
Type: JSON Object
Default: {'description': 'Specifies the default loglevel to be used for subsystems for which no specific loglevel is defined\n-1: Absolutely silent\n0: Very basic auditing logs, (e.g. SA up/SA down)\n1: Generic control flow with errors, a good default to see whats going on\n2: More detailed debugging control flow\n3: Including RAW data dumps in hex\n4: Also include sensitive material in dumps, e.g. keys', 'type': 'integer', 'enum': [-1, 0, 1, 2, 3, 4], 'default': 1}

2.26.1.1.93.2.1 ike_name

Property: VPN :: Modules :: charon-systemd :: syslog :: ^(auth|daemon)$ :: ike_name
Description: Prefix each log entry with the connection name and a unique numerical identifier for each IKE_SA
Type: Boolean true or false.
Default: False

2.26.1.1.93.2.2 log_level

Property: VPN :: Modules :: charon-systemd :: syslog :: ^(auth|daemon)$ :: log_level
Description: Add the log level of each message after the subsystem
Type: Boolean true or false.
Default: False

2.26.1.1.93.2.3 map_level

Property: VPN :: Modules :: charon-systemd :: syslog :: ^(auth|daemon)$ :: map_level
Description: Map strongSwan specific loglevels to syslog loglevels.

The default setting of -1 passes all messages to syslog using a log level of LOG_INFO. A non-negative value maps the strongSwan specific loglevels (0..4) to the syslog level starting at the specified number. For example, a value of 5 (LOG_NOTICE) maps strongSwan loglevel 0 to LOG_NOTICE, level 1 to LOG_INFO, and levels 2, 3 and 4 to LOG_DEBUG. This allows (additional) filtering of log messages on the syslog server.
Type: Integer with a minimum of -1 enum of -1, 0, 1, 2, 3, 4, 5, 6, 7.
Default: -1

2.26.1.1.93.2.4 ^(auth|daemon)$ :: <pattern>

Property: VPN :: Modules :: charon-systemd :: syslog :: ^(auth|daemon)$ :: ^(app|asn|cfg|chd|dmn|enc|esp|ike|job|knl|lib|mgr|net|tls)$
Description: Log level for a specific subsystem
app - applications other than daemons
asn - Low-level encoding/decoding (ASN.1, X.509 etc.)
cfg - Configuration management and plugins
chd - CHILD_SA/IPsec SA
dmn - Main daemon setup/cleanup/signal handling
enc - Packet encoding/decoding encryption/decryption operations
esp - libipsec library messages
ike - IKE_SA/ISAKMP SA
job - Jobs queuing/processing and thread pool management
knl - IPsec/Networking kernel interface
lib - libstrongswan library messages
mgr - IKE_SA manager, handling synchronization for IKE_SA access
net - IKE network communication
tls - libtls library messages
Type: Integer enum of -1, 0, 1, 2, 3, 4.
Default: 1

2.26.1.1.94 threads
Property: VPN :: Modules :: charon-systemd :: threads
Description: Number of worker threads. Several of these are reserved for long running tasks in internal modules and plugins. Therefore, make sure you don't set this value too low.
Type: Integer with a minimum of 1.
Default: 16

2.26.1.1.95 user
Property: VPN :: Modules :: charon-systemd :: user
Description: Name of the user the daemon changes to after startup
Type: String.
Default: None

2.26.1.1.96 x509
Property: VPN :: Modules :: charon-systemd :: x509

Description: X.509 certificate options
Type: JSON Object
Default: None

2.26.1.1.96.1 enforce_critical
Property: VPN :: Modules :: charon-systemd :: x509 :: enforce_critical
Description: Discard certificates with unsupported or unknown critical extensions
Type: Boolean true or false.
Default: True

2.26.1.1.97 plugins
Property: VPN :: Modules :: charon-systemd :: plugins
Description: Charon plugin configurations
Type: JSON Object
Default: None

2.26.1.1.97.1 addrblock
Property: VPN :: Modules :: charon-systemd :: plugins :: addrblock
Description: Implements authorization of remote subnets against the IPAddrBlocks extension as standardized in RFC 3779 that are contained in the peer's X.509 certificate.
Type: JSON Object
Default: None

2.26.1.1.97.1.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: addrblock :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.1.2depth

Property: VPN :: Modules :: charon-systemd :: plugins :: addrblock :: depth
Description: How deep towards the root CA to validate issuer cert IPAddrblock extensions (since version 5.9.6).
RFC 3779 requires that all addrblocks claimed by a certificate must be contained in the IPAddrblock extension of the issuer certificate, up to the root CA. The default depth setting of -1 enforces this.
In practice, third party (root) CAs may not contain the extension, making the IPAddrblock extension unusable under such CAs. By limiting the validation depth, only a certain level of issuer certificates are validated for proper IPAddrblock extensions: A depth of 0 does not check any issuer certificate extensions, a depth of 1 only the direct issuer of the end entity certificate is checked, and so on.
Type: Integer.
Default: -1

2.26.1.1.97.1.3strict

Property: VPN :: Modules :: charon-systemd :: plugins :: addrblock :: strict
Description: If set to true, a subject certificate without an IPAddrblock extension is rejected if the issuer certificate posesses an IPAddrblock extension extension. If set to no, subject certificates issued without the IPAddrblock extension are accepted without any traffic selector checks and no policy is enforced by the plugin.
Type: Boolean true or false.
Default: True

2.26.1.1.97.2 attr
Property: VPN :: Modules :: charon-systemd :: plugins :: attr
Description: IKE attributes to provide to peers
Type: JSON Object
Default: None

2.26.1.1.97.2.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.2.2address

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: address
Description: Internal IPv4 or IPv6 address.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.1.1.97.2.3netmask

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: netmask
Description: Netmask of the internal network (in dotted decimal notation), similar to subnet but bound to the internal address.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.1.1.97.2.4dns

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: dns
Description: List of DNS addresses.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.1.1.97.2.5nbns

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: nbns

Description: List of NBNS/WINS addresses.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.1.1.97.2.6dhcp

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: dhcp
Description: List of DHCP server addresses.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.1.1.97.2.7subnet

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: subnet
Description: The protected sub-networks that this edge-device protects (in CIDR notation: network/mask). Usually ignored in deference to local_ts.
Type: Refer to - definitions->types->IPAddressMaskReqArr
Default: None

2.26.1.1.97.2.8 attr :: <pattern>

Property: VPN :: Modules :: charon-systemd :: plugins :: attr :: ^([1-9]|[1-9][0-9]{1,3}|[12][0-9]{4}|3[01][0-9]{3}|32[0-6][0-9]{2}|327[0-5][0-9]|3276[0-7])$
Description: Numerically identified attribute.
Type: String.
Default: None

2.26.1.1.97.3 bypass-lan

Property: VPN :: Modules :: charon-systemd :: plugins :: bypass-lan
Description: The bypass-lan plugin automatically installs and updates passthrough/bypass policies for locally attached subnets. This is useful for mobile hosts that are used in different networks that want to access local devices in these networks (e.g. printers or NAS) while connected to a VPN that would otherwise cover that traffic too (e.g. if the remote traffic selector is 0.0.0.0/0).
Type: JSON Object
Default: None

2.26.1.1.97.3.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: bypass-lan :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.3.2interfaces_ignore

Property: VPN :: Modules :: charon-systemd :: plugins :: bypass-lan :: interfaces_ignore

Description: A list of network interfaces for which connected subnets should be ignored. If interfaces_use is specified this option has no effect
Type: Array.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.97.3.3interfaces_use

Property: VPN :: Modules :: charon-systemd :: plugins :: bypass-lan :: interfaces_use
Description: A list of network interfaces for which connected subnets should be considered. All other interfaces are ignored
Type: Array.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.97.4 certexpire

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire
Description: Collects expiration dates of all certificates and their trustchain used for authentication. Can export dates to CSV.
Type: JSON Object
Default: None

2.26.1.1.97.4.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.4.2csv

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv
Description: Options used for exporting expiration dates to CSV files
Type: JSON Object
Default: None

2.26.1.1.97.4.2.1 cron

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: cron
Description: Cron style string specifying CSV export times
Type: String.
Default: None

2.26.1.1.97.4.2.2 empty_string

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: empty_string
Description: String to use in empty intermediate CA fields
Type: String.

Default: None

2.26.1.1.97.4.2.3 fixed_fields

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: fixed_fields
Description: Use a fixed intermediate CA field count
Type: Boolean true or false.
Default: True

2.26.1.1.97.4.2.4 format

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: format
Description: strftime() format string to export expiration dates as.
Type: String.
Default: %d:%m:%Y

2.26.1.1.97.4.2.5 local

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: local
Description: strftime() format string for the CSV file to export local certificates to
Type: String.
Default: None

2.26.1.1.97.4.2.6 remote

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: remote
Description: strftime() format string for the CSV file to export remote certificates to
Type: String.
Default: None

2.26.1.1.97.4.2.7 separator

Property: VPN :: Modules :: charon-systemd :: plugins :: certexpire :: csv :: separator
Description: CSV field separator
Type: String with a maximum length of 1.
Default: None

2.26.1.1.97.5 curl

Property: VPN :: Modules :: charon-systemd :: plugins :: curl
Description: curl plugin options
Type: JSON Object
Default: None

2.26.1.1.97.5.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: curl :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.5.2redir

Property: VPN :: Modules :: charon-systemd :: plugins :: curl :: redir
Description: Maximum number of redirects followed by the plugin, set to 0 to disable following redirects, set to -1 for no limit
Type: Integer with a minimum of -1.
Default: -1

2.26.1.1.97.5.3tls_backend

Property: VPN :: Modules :: charon-systemd :: plugins :: curl :: tls_backend
Description: The SSL/TLS backend to configure in curl if multiple are available. A list of available options is logged on level 2 if nothing is configured. Similar but on level 1 if the selected backend isn't available
Type: String enum of openssl.
Default: openssl

2.26.1.1.97.6 dhcp
Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp
Description: The dhcp plugin allows forwarding requests for virtual IP addresses to a DHCPv4 server
Type: JSON Object
Default: None

2.26.1.1.97.6.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.6.2force_server_address

Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp :: force_server_address
Description: Always use the configured server address
Type: Boolean true or false.
Default: False

2.26.1.1.97.6.3identity_lease

Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp :: identity_lease
Description: Derive user-defined MAC address from hash of IKE identity. The client identity DHCP option containing the IKE identity is only sent if this option is enabled
Type: Boolean true or false.
Default: False

2.26.1.1.97.6.4interface

Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp :: interface
Description: Interface name the plugin uses for address allocation. The default is to bind to any (0.0.0.0) and let the system decide which way to route the packets to the DHCP server
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.97.6.5server

Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp :: server
Description: DHCP server unicast or broadcast IP address
Type: Refer to - definitions->types->IPv4Address
Default: 255.255.255.255

2.26.1.1.97.6.6use_server_port

Property: VPN :: Modules :: charon-systemd :: plugins :: dhcp :: use_server_port
Description: Use the DHCP server port 67 as source port instead of the DHCP client port 68 when a unicast server address is configured and the plugin acts as relay agent
Type: Boolean true or false.
Default: False

2.26.1.1.97.7 eap-aka
Property: VPN :: Modules :: charon-systemd :: plugins :: eap-aka
Description: EAP-AKA authentication plugin
Type: JSON Object
Default: None

2.26.1.1.97.7.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-aka :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.7.2request_identity

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-aka :: request_identity
Type: Boolean true or false.
Default: True

2.26.1.1.97.8 eap-dynamic
Property: VPN :: Modules :: charon-systemd :: plugins :: eap-dynamic
Description: EAP-Dynamic authentication plugin
Type: JSON Object
Default: None

2.26.1.1.97.8.1load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-dynamic :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.8.2 prefer_user

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-dynamic :: prefer_user
Description: If enabled the order of the EAP methods in an EAP-NAK message sent by a client is preferred over the one configured locally
Type: Boolean true or false.
Default: False

2.26.1.1.97.8.3 preferred

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-dynamic :: preferred
Description: The preferred EAP method(s) to be used. If not set, the first registered method will be used initially. If multiple methods are listed, the methods are tried in the given order before trying the rest of the registered methods
Type: Array.
Item type: String enum of aka, gtc, md5, mschapv2, peap, tls, ttls.
Default: None

2.26.1.1.97.9 eap-gtc

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-gtc
Description: EAP-GTC authentication plugin
Type: JSON Object
Default: None

2.26.1.1.97.9.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-gtc :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.9.2 backend

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-gtc :: backend
Description: XAuth backend to use
Type: String enum of eap, pam, generic.
Default: pam

2.26.1.1.97.10 eap-peap

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap
Description: EAP-PEAP authentication plugin

Type: JSON Object
Default: None

2.26.1.1.97.10.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.10.2 fragment_size

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: fragment_size
Description: Maximum size of an EAP-PEAP packet
Type: Integer with a minimum of 0.
Default: 1024

2.26.1.1.97.10.3 include_length

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: include_length
Description: Include length in non-fragmented EAP-PEAP packets
Type: Boolean true or false.
Default: True

2.26.1.1.97.10.4 max_message_count

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: max_message_count
Description: Maximum number of processed EAP-PEAP packets (0 = no limit)
Type: Integer with a minimum of 0.
Default: 32

2.26.1.1.97.10.5 phase2_method

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: phase2_method
Description: Phase2 EAP client authentication method
Type: String enum of aka, gtc, md5, mschapv2, peap, tls, ttls.
Default: mschapv2

2.26.1.1.97.10.6 phase2_piggyback

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: phase2_piggyback
Description: Phase2 EAP Identity request piggybacked by server onto TLS Finished message
Type: Boolean true or false.
Default: False

2.26.1.1.97.10.7 request_peer_auth

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-peap :: request_peer_auth
Description: Request peer authentication based on a client certificate

Type: Boolean true or false.
Default: False

2.26.1.1.97.11 eap-radius
Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius
Description: RADIUS proxy authentication plugin for EAP
Type: JSON Object
Default: None

2.26.1.1.97.11.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.11.2 accounting

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: accounting
Description: Enable EAP-RADIUS accounting
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.3 accounting_close_on_timeout

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: accounting_close_on_timeout
Description: Close the IKE_SA if there is a timeout during interim RADIUS accounting updates
Type: Boolean true or false.
Default: True

2.26.1.1.97.11.4 accounting_interval

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: accounting_interval
Description: Interval in seconds for interim RADIUS accounting updates, if not specified by the RADIUS server in the Access-Accept message
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.97.11.5 accounting_requires_vip

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: accounting_requires_vip
Description: If enabled, accounting is disabled unless an IKE_SA has at least one virtual IP
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.6 accounting_send_class

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: accounting_send_class
Description: If enabled, adds the Class attributes received in Access-Accept message to the RADIUS accounting messages
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.7 class_group

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: class_group
Description: Use the class attribute sent in the Access-Accept message as group membership information.
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.8 close_all_on_timeout

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: close_all_on_timeout
Description: Closes all IKE_SAs if communication with the RADIUS server times out. If it is not set only the current IKE_SA is closed
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.9 dae

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: dae
Description: Dynamic Authorization Extension
Type: JSON Object
Default: None

2.26.1.1.97.11.9.1 enable

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: dae :: enable
Description: Enables support for the Dynamic Authorization Extension
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.9.2 listen

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: dae :: listen
Description: Address to listen for DAE messages from the RADIUS server
Type: Refer to - definitions->types->IPAddress
Default: 0.0.0.0

2.26.1.1.97.11.9.3 port

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: dae :: port
Description: Port to listen for DAE requests
Type: Refer to - definitions->types->Port
Default: 3799

2.26.1.1.97.11.9.4 secret

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: dae :: secret
Description: Shared secret used to verify/sign DAE messages
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.1.1.97.11.10 eap_start

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: eap_start
Description: Send EAP-Start instead of EAP-Identity to start RADIUS conversation
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.11 filter_id

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: filter_id
Description: Use the filter_id attribute sent in the RADIUS-Accept message as group membership if the RADIUS tunnel_type attribute is set to ESP
Type: Boolean true or false.
Default: False

2.26.1.1.97.11.12 forward

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: forward
Description: Attributes to forward between IKEv2 and RADIUS
Type: Boolean true or false.
Default: None

2.26.1.1.97.11.12.1 ike_to_radius

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: forward :: ike_to_radius
Description: RADIUS attributes to be forwarded from IKEv2 to RADIUS (can be defined by name or attribute number, a colon can be used to specify vendor-specific attributes, e.g. Reply-Message, or 11, or 36906:12)
Type: Array.
Item type: String.
Default: None

2.26.1.1.97.11.12.2 radius_to_ike

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: forward :: radius_to_ike
Description: Same as above but from RADIUS to IKEv2, a strongSwan specific private notify (40969) is used to transmit the attributes
Type: Array.
Item type: String.
Default: None

2.26.1.1.97.11.13 id_prefix

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: id_prefix

Description: Prefix to EAP-Identity, some AAA servers use a IMSI prefix to select the EAP method
Type: String.
Default: None

2.26.1.1.97.11.14 nas_identifier

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: nas_identifier
Description: NAS-Identifier to include in RADIUS messages.
Type: String.
Default: strongSwan

2.26.1.1.97.11.15 port

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: port
Description: Port of RADIUS server (authentication)
Type: Refer to - definitions->types->Port
Default: 1812

2.26.1.1.97.11.16 retransmit_base

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: retransmit_base
Description: Base to use for calculating exponential back off
Type: Number.
Default: 1.4

2.26.1.1.97.11.17 retransmit_timeout

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: retransmit_timeout
Description: Timeout in seconds before sending first retransmit
Type: Number.
Default: 2.0

2.26.1.1.97.11.18 retransmit_tries

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: retransmit_tries
Description: Number of times to retransmit a packet before giving up
Type: Integer with a minimum of 0.
Default: 4

2.26.1.1.97.11.19 secret

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: secret
Description: Shared secret between RADIUS and NAS.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.1.1.97.11.20 server

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: server

Description: IP/Hostname of RADIUS server
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.26.1.1.97.11.21 servers

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers
Description: Section to specify multiple RADIUS servers.
Type: JSON Object
Default: None

2.26.1.1.97.11.21.1 servers :: <pattern>

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$
Description: Configuration of a single RADIUS server
Type: JSON Object
Default: None

2.26.1.1.97.11.21.1.1 address

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: address
Description: IP/Hostname of RADIUS server
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.26.1.1.97.11.21.1.2 nas_identifier

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: nas_identifier
Description: NAS-Identifier to include in RADIUS messages.
Type: String.
Default: strongSwan

2.26.1.1.97.11.21.1.3 auth_port

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: auth_port
Description: Port of RADIUS server (authentication)
Type: Refer to - definitions->types->Port
Default: 1812

2.26.1.1.97.11.21.1.4 acct_port

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: acct_port
Description: Port of RADIUS server (accounting)
Type: Refer to - definitions->types->Port
Default: 1813

2.26.1.1.97.11.21.1.5 preference

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: preference
Description: Used to set priority for a specific server (higher=preferred). Defining a preference of 110 or more is not a good idea, such a server will always win the election process even if unavailable.
Type: Integer with a minimum of 0 and a maximum of 200.
Default: None

2.26.1.1.97.11.21.1.6 retransmit_base

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: retransmit_base
Description: Base to use for calculating exponential back off
Type: Number.
Default: 1.4

2.26.1.1.97.11.21.1.7 retransmit_timeout

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: retransmit_timeout
Description: Timeout in seconds before sending first retransmit
Type: Number.
Default: 2.0

2.26.1.1.97.11.21.1.8 retransmit_tries

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: retransmit_tries
Description: Number of times to retransmit a packet before giving up
Type: Integer with a minimum of 0.
Default: 4

2.26.1.1.97.11.21.1.9 secret

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Shared secret between RADIUS and NAS.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.1.1.97.11.21.1.10 sockets

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: servers :: ^[a-zA-Z0-9_-]{0,20}$ :: sockets
Description: Number of sockets (ports) to use. Increase for high load
Type: Integer with a minimum of 1.
Default: 1

2.26.1.1.97.11.22 sockets

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: sockets
Description: Number of sockets (ports) to use. Increase for high load
Type: Integer with a minimum of 1.
Default: 1

2.26.1.1.97.11.23 station_id_with_port

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: station_id_with_port
Description: Whether to include the UDP port in the Called-Station_ID and Calling-Station-Id attributes
Type: Boolean true or false.
Default: True

2.26.1.1.97.11.24 xauth

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: xauth
Description: Section to configure multiple XAuth authentication rounds via RADIUS
Type: JSON Object
Default: None

2.26.1.1.97.11.24.1 xauth :: <pattern>

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: xauth :: ^[a-zA-Z0-9_-]{0,20}$
Description: Configuration of a single XAuth round. Replies are concatenated to the User-Password attribute
Type: JSON Object
Default: None

2.26.1.1.97.11.24.1.1 answer

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: xauth :: ^[a-zA-Z0-9_-]{0,20}$ :: answer
Description: Prompt for message-answer
Type: String.
Default: None

2.26.1.1.97.11.24.1.2 nextpin

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: xauth :: ^[a-zA-Z0-9_-]{0,20}$ :: nextpin
Description: Prompt for next pin

Type: String.
Default: None

2.26.1.1.97.11.24.1.3 passcode

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: xauth :: ^[a-zA-Z0-9_-]{0,20}$ :: passcode
Description: Prompt for passcode
Type: String.
Default: None

2.26.1.1.97.11.24.1.4 password

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-radius :: xauth :: ^[a-zA-Z0-9_-]{0,20}$ :: password
Description: Prompt for password
Type: String.
Default: None

2.26.1.1.97.12 eap-tls

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-tls
Description: EAP-TLS authentication plugin
Type: JSON Object
Default: None

2.26.1.1.97.12.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-tls :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.12.2 fragment_size

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-tls :: fragment_size
Description: Maximum size of an EAP-TLS packet
Type: Integer with a minimum of 0.
Default: 1024

2.26.1.1.97.12.3 include_length

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-tls :: include_length
Description: Include length in non-fragmented EAP-TLS packets
Type: Boolean true or false.
Default: True

2.26.1.1.97.12.4 max_message_count

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-tls :: max_message_count

Description: Maximum number of processed EAP-TLS packets (0 = no limit)
Type: Integer with a minimum of 0.
Default: 32

2.26.1.1.97.13 eap-ttls
Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls
Description: EAP-TTLS authentication plugin
Type: JSON Object
Default: None

2.26.1.1.97.13.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.13.2 fragment_size

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: fragment_size
Description: Maximum size of an EAP-TTLS packet
Type: Integer with a minimum of 0.
Default: 1024

2.26.1.1.97.13.3 include_length

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: include_length
Description: Include length in non-fragmented EAP-TTLS packets
Type: Boolean true or false.
Default: True

2.26.1.1.97.13.4 max_message_count

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: max_message_count
Description: Maximum number of processed EAP-TTLS packets (0 = no limit)
Type: Integer with a minimum of 0.
Default: 32

2.26.1.1.97.13.5 phase2_method

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: phase2_method
Description: Phase2 EAP client authentication method
Type: String enum of aka, gtc, md5, mschapv2, peap, tls, ttls.
Default: md5

2.26.1.1.97.13.6 phase2_piggyback

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: phase2_piggyback

Description: Phase2 EAP Identity request piggybacked by server onto TLS Finished message
Type: Boolean true or false.
Default: False

2.26.1.1.97.13.7 request_peer_auth

Property: VPN :: Modules :: charon-systemd :: plugins :: eap-ttls :: request_peer_auth
Description: Request peer authentication based on a client certificate
Type: Boolean true or false.
Default: False

2.26.1.1.97.14 forecast
Property: VPN :: Modules :: charon-systemd :: plugins :: forecast
Description: The forecast plugin uses Linux Netfilter marks to allow identical IPsec policies having multicast or broadcast selectors and uses a listen-and-forward mechanism to forward such traffic over all matching SAs. It supports forwarding of multi/broadcast traffic between multiple connected clients and between clients and a LAN attached to the IPsec gateway.
Type: JSON Object
Default: None

2.26.1.1.97.14.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: forecast :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.14.2 groups

Property: VPN :: Modules :: charon-systemd :: plugins :: forecast :: groups
Description: List of multicast groups to join locally. The local host receives and forwards packets in the local LAN for joined multicast groups only. Packets matching the list of multicast groups get forwarded to connected clients. The default group includes host multicasts, IGMP, mDNS, LLMNR and SSDP/WS-Discovery and is usually a good choice for Windows clients.
Type: Array.
Type: Refer to - definitions->types->IPv4Multicast
Default: None

2.26.1.1.97.14.3 interface

Property: VPN :: Modules :: charon-systemd :: plugins :: forecast :: interface
Description: Name of the local interface to listen for broadcasts messages to forward. If no interface is configured, the first usable interface is used, which is usually just fine for single-homed hosts. If your host has multiple interfaces, set this option to the local LAN interface you want to forward broadcasts from/to.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.26.1.1.97.14.4 reinject

Property: VPN :: Modules :: charon-systemd :: plugins :: forecast :: reinject
Description: List of CHILD SA configuration names for which to perform multi/broadcast reinjection. For clients connecting over such a configuration, any multi/broadcast received over the tunnel gets reinjected to all active tunnels. This makes the broadcasts visible to other peers, and for examples allows clients to see others shares. If disabled, multi/broadcast messages received over a tunnel are injected to the local network only, but not to other IPsec clients.
Type: Array.
Item type: String pattern of ^[a-zA-Z0-9_-]+$.
Default: None

2.26.1.1.97.15 ha

Property: VPN :: Modules :: charon-systemd :: plugins :: ha
Description: The ha plugin supports active/passive High Availability and active/active Load Sharing capabilities using a cluster of two nodes.
Type: JSON Object
Default: None

2.26.1.1.97.15.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.15.2 autobalance

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: autobalance
Description: Interval in seconds to automatically balance handled segments between nodes. Set to 0 to disable
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.97.15.3 buflen

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: buflen
Description: Buffer size for received HA messages. For IKEv1 the public DH factors are also transmitted so depending on the DH group the HA messages can get quite big (the default should be fine up to modp4096)
Type: Integer with a minimum of 0.
Default: 2048

2.26.1.1.97.15.4 fifo_interface

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: fifo_interface
Description: Enable the segment responsibility administration interface

Type: Boolean true or false.
Default: True

2.26.1.1.97.15.5 heartbeat_delay

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: heartbeat_delay
Description: Time between heartbeats
Type: Integer with a minimum of 0.
Default: 1000

2.26.1.1.97.15.6 heartbeat_timeout

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: heartbeat_timeout
Description: Time after the last received heartbeat after which a failure is declared.
Type: Integer with a minimum of 0.
Default: 2100

2.26.1.1.97.15.7 local

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: local
Description: IP address on which to receive sync messages
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.1.1.97.15.8 monitor

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: monitor
Description: Enable the heartbeat based remote node monitoring
Type: Boolean true or false.
Default: True

2.26.1.1.97.15.9 pools

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: pools
Description: Optional HA-enabled virtual IP address pool subsection
Type: JSON Object
Default: None

2.26.1.1.97.15.9.1 pools :: <pattern>

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: pools :: ^[a-zA-Z0-9_-]{0,20}$
Description: HA-enabled virtual IP address pool shared between HA cluster nodes
Type: Refer to - definitions->types->IPAddressMaskReq
Default: None

2.26.1.1.97.15.10 remote

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: remote
Description: IP address to send sync messages to
Type: Refer to - definitions->types->IPAddress

Default: None

2.26.1.1.97.15.11 resync

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: resync
Description: Enable automatic state resynchronization if a node joins the cluster
Type: Boolean true or false.
Default: True

2.26.1.1.97.15.12 secret

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: secret
Description: If specified, the nodes automatically establish a pre-shared key authenticated IPsec tunnel for HA sync and control messages
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.1.1.97.15.13 segment_count

Property: VPN :: Modules :: charon-systemd :: plugins :: ha :: segment_count
Description: Number of ClusterIP segments to use
Type: Integer with a minimum of 0.
Default: 1

2.26.1.1.97.16 kernel-netlink
Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink
Description: Netlink kernel interface plugin
Type: JSON Object
Default: None

2.26.1.1.97.16.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.16.2 buflen

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: buflen
Description: Buffer size for received Netlink messages. Default is calculated as min(PAGE_SIZE, 8192)
Type: Integer with a minimum of 0.
Default: None

2.26.1.1.97.16.3 force_receive_buffer_size

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: force_receive_buffer_size
Description: If the maximum Netlink socket receive buffer in bytes set by receive_buffer_size exceeds the system-wide maximum from /proc/sys/net/core/rmem_max, this option can be used to override the limit. Enabling this option requires special privileges (CAP_NET_ADMIN)
Type: Boolean true or false.
Default: False

2.26.1.1.97.16.4 fwmark

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: fwmark
Description: Firewall mark to set on the routing rule that directs traffic to our own routing table. The format is [!]mark[/mask], where the optional exclamation mark inverts the meaning (i.e. the rule only applies to packets that don't match the mark). A possible use case is host-to-host tunnels with kernel-libipsec. When set to !<mark> a more efficient lookup for source and next-hop addresses may also be used.
Type: String.
Default: None

2.26.1.1.97.16.5 hw_offload_feature_interface

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: hw_offload_feature_interface
Description: If the kernel supports hardware offloading, the plugin needs to find the feature flag which represents hardware offloading support for network devices. Using the loopback device for this purpose is usually fine, since it should always be present. For rare cases in which the loopback device cannot be used to obtain the appropriate feature flag, this option can be used to specify an alternative interface for offload feature detection
Type: Refer to - definitions->types->InterfaceName
Default: lo

2.26.1.1.97.16.6 install_routes_xfrmi

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: install_routes_xfrmi
Description: Whether routes via XFRM interfaces are automatically installed for SAs that reference such an interface via if_id_out. If the traffic selectors include the IKE traffic to the peer, this requires special care (e.g. installing bypass policies and/or routes, or setting a mark on the IKE socket and excluding such packets from the configured routing table via fwmark option).
Type: Boolean true or false.
Default: False

2.26.1.1.97.16.7 mss

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: mss
Description: MSS to set on installed routes, 0 to disable
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.97.16.8 mtu

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: mtu
Description: MTU to set on installed routes, 0 to disable
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.97.16.9 process_rules

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: process_rules
Description: Whether to process changes in routing rules to trigger roam events. This is currently only useful if the kernel based route lookup is used (i.e. if route installation is disabled or an inverted fwmark match is configured)
Type: Boolean true or false.
Default: False

2.26.1.1.97.16.10 receive_buffer_size

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: receive_buffer_size
Description: Maximum Netlink socket receive buffer in bytes. This value controls how many bytes of Netlink messages can be received on a Netlink socket. The default value is set by /proc/sys/net/core/rmem_default. The specified value cannot exceed the system-wide maximum from /proc/sys/net/core/rmem_max unless force_receive_buffer_size is enabled
Type: Integer with a minimum of 0.
Default: 0

2.26.1.1.97.16.11 roam_events

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: roam_events
Description: Whether to trigger roam events when interfaces, addresses or routes change
Type: Boolean true or false.
Default: True

2.26.1.1.97.16.12 set_proto_port_transport_sa

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: set_proto_port_transport_sa
Description: Whether to set protocol and ports in the selector installed on transport mode IPsec SAs in the kernel. While doing so enforces policies for inbound traffic, it also prevents the use of a single IPsec SA by more than one traffic selector
Type: Boolean true or false.
Default: False

2.26.1.1.97.16.13 spdh_thresh

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh
Description: Subsection to configure XFRM policy hashing thresholds for IPv4 and IPv6. The section defines hashing thresholds to configure in the kernel during daemon startup. Each address family takes a threshold for the local subnet of an IPsec policy (src in out-policies, dst in

in- and forward-policies) and the remote subnet (dst in out-policies, src in in- and forward-policies). If the subnet has more or equal net bits than the threshold, the first threshold bits are used to calculate a hash to lookup the policy. Note: These settings are mostly obsolete since Linux 5.0, which started using a multi-level tree-based policy lookup.
Type: JSON Object
Default: None

2.26.1.1.97.16.13.1 ipv4

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh :: ipv4
Type: JSON Object
Default: None

2.26.1.1.97.16.13.1.1 lbits

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh :: ipv4 :: lbits
Description: Local subnet XFRM policy hashing threshold for IPv4
Type: Integer with a minimum of 0.
Default: 32

2.26.1.1.97.16.13.1.2 rbits

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh :: ipv4 :: rbits
Description: Remote subnet XFRM policy hashing threshold for IPv4
Type: Integer with a minimum of 0.
Default: 32

2.26.1.1.97.16.13.2 ipv6

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh :: ipv6
Type: JSON Object
Default: None

2.26.1.1.97.16.13.2.1 lbits

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh :: ipv6 :: lbits
Description: Local subnet XFRM policy hashing threshold for IPv6
Type: Integer with a minimum of 0.
Default: 128

2.26.1.1.97.16.13.2.2 rbits

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: spdh_thresh :: ipv6 :: rbits
Description: Remote subnet XFRM policy hashing threshold for IPv6
Type: Integer with a minimum of 0.
Default: 128

2.26.1.1.97.16.14 xfrm_acq_expires

Property: VPN :: Modules :: charon-systemd :: plugins :: kernel-netlink :: xfrm_acq_expires
Description: Lifetime of XFRM acquire state created by the kernel when traffic matches a trap policy. Indirectly controls the delay between XFRM acquire messages triggered by the kernel for a trap policy. The same value is used as timeout for SPIs allocated by the kernel. The default value equals the default total retransmission timeout for IKE messages (since version 5.5.3 this value is determined dynamically based on the configuration)
Type: Integer with a minimum of 0.
Default: 165

2.26.1.1.97.17 led

Property: VPN :: Modules :: charon-systemd :: plugins :: led
Description: Let Linux LED subsystem LEDs blink on IKE activity
Type: JSON Object
Default: None

2.26.1.1.97.17.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: led :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.17.2 activity_led

Property: VPN :: Modules :: charon-systemd :: plugins :: led :: activity_led
Type: Boolean true or false.
Default: None

2.26.1.1.97.17.3 blink_time

Property: VPN :: Modules :: charon-systemd :: plugins :: led :: blink_time
Type: Integer with a minimum of 0.
Default: 50

2.26.1.1.97.18 openssl

Property: VPN :: Modules :: charon-systemd :: plugins :: openssl
Description: OpenSSL crypto plugin
Type: JSON Object
Default: None

2.26.1.1.97.18.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: openssl :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.

Type: Boolean true or false.
Default: True

2.26.1.1.97.18.2 engine_id

Property: VPN :: Modules :: charon-systemd :: plugins :: openssl :: engine_id
Description: ENGINE ID to use in the OpenSSL plugin.
Type: String.
Default: pkcs11

2.26.1.1.97.18.3 fips_mode

Property: VPN :: Modules :: charon-systemd :: plugins :: openssl :: fips_mode
Description: Set OpenSSL FIPS mode. Any value other than 0 (disabled) will explicitly load the fips and base providers (load_legacy will be ignored). The latter still requires the config in fipsmodule.cnf (e.g. for the module's MAC), but allows explicitly loading the provider if it's not activated in that config
Type: Integer.
Default: 0

2.26.1.1.97.18.4 load_legacy

Property: VPN :: Modules :: charon-systemd :: plugins :: openssl :: load_legacy
Description: Load the legacy provider for algorithms like MD4, DES, or Blowfish (the first two are required for EAP-MSCHAPv2). If disabled, the default provider is loaded, or those configured in the OpenSSL config (e.g. the fips provider)
Type: Boolean true or false.
Default: True

2.26.1.1.97.19 pkcs11
Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11
Description: PKCS#11 crypto token support plugin
Type: JSON Object
Default: None

2.26.1.1.97.19.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.19.2 modules

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: modules
Description: Subsection listing available PKCS#11 modules
Type: JSON Object
Default: None

2.26.1.1.97.19.2.1 modules :: <pattern>

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: modules :: ^[a-zA-Z0-9_-]{0,30}$
Description: Options for a specific PKCS#11 module
Type: JSON Object
Default: None

2.26.1.1.97.19.2.1.1 path

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: modules :: ^[a-zA-Z0-9_-]{0,30}$ :: path
Description: Full path to the shared object file of this PKCS#11 module
Type: Refer to - definitions->types->File_Dir
Default: None

2.26.1.1.97.19.2.1.2 os_locking

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: modules :: ^[a-zA-Z0-9_-]{0,30}$ :: os_locking
Description: Whether OS locking should be enabled for this module
Type: Boolean true or false.
Default: False

2.26.1.1.97.19.2.1.3 load_certs

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: modules :: ^[a-zA-Z0-9_-]{0,30}$ :: load_certs
Description: Whether the PKCS#11 modules should load certificates from tokens
Type: Boolean true or false.
Default: True

2.26.1.1.97.19.3 reload_certs

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: reload_certs
Description: Whether the PKCS#11 modules should reload all certificates if charon receives a SIGHUP signal
Type: Boolean true or false.
Default: False

2.26.1.1.97.19.4 use_dh

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: use_dh
Description: Whether the PKCS#11 modules should be used for DH and ECDH
Type: Boolean true or false.
Default: False

2.26.1.1.97.19.5 use_ecc

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: use_ecc

Description: Whether the PKCS#11 modules should be used for ECDH and ECDSA public key operations. ECDSA private keys can be used regardless of this option
Type: Boolean true or false.
Default: False

2.26.1.1.97.19.6 use_hasher

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: use_hasher
Description: Whether the PKCS#11 modules should be used to hash data
Type: Boolean true or false.
Default: False

2.26.1.1.97.19.7 use_pubkey

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: use_pubkey
Description: Whether the PKCS#11 modules should be used for public key operations, even for keys not stored on tokens
Type: Boolean true or false.
Default: False

2.26.1.1.97.19.8 use_rng

Property: VPN :: Modules :: charon-systemd :: plugins :: pkcs11 :: use_rng
Description: Whether the PKCS#11 modules should be used as RNG
Type: Boolean true or false.
Default: False

2.26.1.1.97.20 resolve
Property: VPN :: Modules :: charon-systemd :: plugins :: resolve
Description: The resolve plugin writes name servers received via configuration payloads (IKEv2) or Mode Config (IKEv1) to resolv.conf
Type: JSON Object
Default: None

2.26.1.1.97.20.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: resolve :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.20.2 resolveconf

Property: VPN :: Modules :: charon-systemd :: plugins :: resolve :: resolveconf
Type: JSON Object
Default: None

2.26.1.1.97.20.2.1 iface

Property: VPN :: Modules :: charon-systemd :: plugins :: resolve :: resolveconf :: iface
Description: The interface name and protocol sent to resolvconf(8). This has to be a valid interface name according to the rules defined by resolvconf. Also, it should have a high priority according to the order defined in interface-order(8) if relevant on the system
Type: String.
Default: lo.inet

2.26.1.1.97.21 revocation
Property: VPN :: Modules :: charon-systemd :: plugins :: revocation
Description: X.509 CRL/OCSP revocation check plugin
Type: JSON Object
Default: None

2.26.1.1.97.21.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: revocation :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.21.2 enable_crl

Property: VPN :: Modules :: charon-systemd :: plugins :: revocation :: enable_crl
Description: Whether CRL validation should be enabled
Type: Boolean true or false.
Default: True

2.26.1.1.97.21.3 enable_ocsp

Property: VPN :: Modules :: charon-systemd :: plugins :: revocation :: enable_ocsp
Description: Whether OCSP validation should be enabled
Type: Boolean true or false.
Default: True

2.26.1.1.97.21.4 timeout

Property: VPN :: Modules :: charon-systemd :: plugins :: revocation :: timeout
Description: Validation timeout in seconds
Type: Integer.
Default: 10

2.26.1.1.97.22 socket-default
Property: VPN :: Modules :: charon-systemd :: plugins :: socket-default
Description: Default socket implementation for charon daemon
Type: JSON Object
Default: None

2.26.1.1.97.22.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: socket-default :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.22.2 set_source

Property: VPN :: Modules :: charon-systemd :: plugins :: socket-default :: set_source
Description: Set source address on outbound packets, if possible
Type: Boolean true or false.
Default: True

2.26.1.1.97.22.3 set_sourceif

Property: VPN :: Modules :: charon-systemd :: plugins :: socket-default :: set_sourceif
Description: Force sending interface on outbound packets, if possible. This allows using IPv6 link-local addresses as tunnel endpoints
Type: Boolean true or false.
Default: False

2.26.1.1.97.22.4 use_ipv4

Property: VPN :: Modules :: charon-systemd :: plugins :: socket-default :: use_ipv4
Description: Listen on IPv4, if possible
Type: Boolean true or false.
Default: True

2.26.1.1.97.22.5 use_ipv6

Property: VPN :: Modules :: charon-systemd :: plugins :: socket-default :: use_ipv6
Description: Listen on IPv6, if possible
Type: Boolean true or false.
Default: True

2.26.1.1.97.23 tpm
Property: VPN :: Modules :: charon-systemd :: plugins :: tpm
Description: Allows to access persistent RSA and ECDSA private keys bound to a TPM 2.0. Optionally, the TPM 2.0 can be enabled as a true random number source.
Keys bound to a TPM 2.0 can only be used with IKEv2, because IKEv1's legacy signature schemes are not supported.
Type: JSON Object
Default: None

2.26.1.1.97.23.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: load

Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.23.2 ek_handle

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: ek_handle
Description: Handle of the RSA or ECC Endorsement Key (EK) to be used to set up an authenticated session with a TPM 2.0 (e.g. 0x81010001)
Type: String pattern of ^0x[a-fA-F0-9]+$.
Default: None

2.26.1.1.97.23.3 fips_186_4

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: fips_186_4
Description: Is the TPM 2.0 FIPS-186-4 compliant, which forces e.g. the use of the default salt length instead of maximum salt length with RSA-PSS padding
Type: Boolean true or false.
Default: False

2.26.1.1.97.23.4 tcti

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: tcti
Description: TPM Command Transmission Interface (TCTI) options
Type: JSON Object
Default: None

2.26.1.1.97.23.4.1 name

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: tcti :: name
Description: Name of TPM 2.0 TCTI library. Valid values: device or tabrmd. Defaults are device if the /dev/tpmrm0 in-kernel TPM 2.0 resource manager device exists and tabrmd otherwise, requiring the D-Bus based TPM 2.0 access broker and resource manager to be available.
Type: String enum of device, tabrmd.
Default: None

2.26.1.1.97.23.4.2 opts

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: tcti :: opts
Description: Options for the TPM 2.0 TCTI library. Defaults are /dev/tpmrm0 if the TCTI library name is device and no options otherwise.
Type: String.
Default: /dev/tpmrm0

2.26.1.1.97.23.5 use_rng

Property: VPN :: Modules :: charon-systemd :: plugins :: tpm :: use_rng
Description: Whether the TPM 2.0 should be used as RNG. For security reasons enable only if an authenticated session can be set up (see ek_handle option)

Type: Boolean true or false.
Default: False

2.26.1.1.97.24 updown
Property: VPN :: Modules :: charon-systemd :: plugins :: updown
Description: updown firewall script plugin
Type: JSON Object
Default: None

2.26.1.1.97.24.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: updown :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.24.2 dns_handler

Property: VPN :: Modules :: charon-systemd :: plugins :: updown :: dns_handler
Description: Whether the updown script should handle DNS servers assigned via IKEv1 ModeConfig or IKEv2 CP Config Payloads. If enabled they can't be handled by other plugins, like resolve
Type: Boolean true or false.
Default: False

2.26.1.1.97.25 xauth-eap
Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-eap
Description: XAuth backend plugin using EAP methods to verify passwords
Type: JSON Object
Default: None

2.26.1.1.97.25.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-eap :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.25.2 backend

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-eap :: backend
Description: EAP plugin to use
Type: String enum of aka, gtc, md5, mschapv2, radius, tls, ttls.
Default: radius

2.26.1.1.97.26 xauth-pam

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-pam
Description: XAuth backend plugin using PAM to verify passwords
Type: JSON Object
Default: None

2.26.1.1.97.26.1 load

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-pam :: load
Description: Whether to load this plugin or not. Exact behavior depends on whether load_modular is enabled.
Type: Boolean true or false.
Default: True

2.26.1.1.97.26.2 pam_service

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-pam :: pam_service
Description: PAM service to use for authentication
Type: String.
Default: login

2.26.1.1.97.26.3 session

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-pam :: session
Description: Open/close a PAM session for each active IKE_SA
Type: Boolean true or false.
Default: False

2.26.1.1.97.26.4 trim_email

Property: VPN :: Modules :: charon-systemd :: plugins :: xauth-pam :: trim_email
Description: If an email address is received as an XAuth username, trim it to just the username part
Type: Boolean true or false.
Default: True

2.26.1.2 libtls
Property: VPN :: Modules :: libtls
Description: TLS cipher suite configuration. Usually unnecessary to modify; the TLS stack enables all secure algorithms it has registered crypto backends for.
Type: JSON Object
Default: None

2.26.1.2.1 cipher
Property: VPN :: Modules :: libtls :: cipher
Description: List of TLS encryption ciphers. NULL encryption is automatically disabled if the stack is used for purposes other than EAP-TLS where only the handshake of TLS is used.
Type: Array.

Item type: String enum of aes256gcm, aes128gcm, chacha20_poly1305, aes128ccm, aes128ccm8, aes256, aes128, camellia256, camellia128, null.
Default: None

2.26.1.2.2 key_exchange
Property: VPN :: Modules :: libtls :: key_exchange
Description: List of TLS key exchange methods
Type: Array.
Item type: String enum of ecdhe-ecdsa, ecdhe-rsa, dhe-rsa, rsa.
Default: None

2.26.1.2.3 ke_group
Property: VPN :: Modules :: libtls :: ke_group
Description: List of TLS key exchange groups
Type: Array.
Item type: String enum of curve448, curve25519, ecp521, ecp384, ecp256, ecp224, ecp192.
Default: None

2.26.1.2.4 mac
Property: VPN :: Modules :: libtls :: mac
Description: List of TLS MAC algorithms
Type: Array.
Item type: String enum of sha384, sha256, sha1.
Default: None

2.26.1.2.5 signature
Property: VPN :: Modules :: libtls :: signature
Description: List of TLS signature schemes
Type: Array.
Item type: String enum of ed448, ed25519, ecdsa_sha512, ecdsa_sha384, ecdsa_sha256, rsa_pss_rsae_sha512, rsa_pss_rsae_sha384, rsa_pss_rsae_sha256, rsa_pkcs1_sha512, rsa_pkcs1_sha384, rsa_pkcs1_sha256.
Default: None

2.26.1.2.6 suites
Property: VPN :: Modules :: libtls :: suites
Description: List of specific TLS cipher suites to use
Type: Array.
Item type: String enum of TLS_AES_256_GCM_SHA384, TLS_AES_128_GCM_SHA256, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_CCM_SHA256, TLS_AES_128_CCM_8_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256,
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256,
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256,
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA,
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256,
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_NULL_SHA,
TLS_ECDHE_RSA_WITH_NULL_SHA, TLS_RSA_WITH_NULL_SHA256,
TLS_RSA_WITH_NULL_SHA.
Default: None

2.26.1.2.7 send_certreq_authorities

Property: VPN :: Modules :: libtls :: send_certreq_authorities
Description: Whether to include CAs in a server's CertificateRequest message. May be disabled if clients can't handle a long list of CAs
Type: Boolean true or false.
Default: True

2.26.1.2.8 version_min

Property: VPN :: Modules :: libtls :: version_min
Description: Minimum TLS version to negotiate. 1.0 and 1.1 are supported but should not be used unless absolutely necessary due to security reasons
Type: String enum of 1.0, 1.1, 1.2, 1.3.
Default: 1.2

2.26.1.2.9 version_max

Property: VPN :: Modules :: libtls :: version_max

Description: Maximum TLS version to negotiate
Type: String enum of 1.0, 1.1, 1.2, 1.3.
Default: 1.2

2.26.1.3 pki
Property: VPN :: Modules :: pki
Description: Options for pki command suite
Type: JSON Object
Default: None

2.26.1.3.1 scep
Property: VPN :: Modules :: pki :: scep
Description: Options for Simple Certificate Enrollment Protocol (SCEP) server operations
Type: JSON Object
Default: None

2.26.1.3.1.1http_bind
Property: VPN :: Modules :: pki :: scep :: http_bind
Description: Source IP address to bind for HTTP operations
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.1.3.1.2http_timeout
Property: VPN :: Modules :: pki :: scep :: http_timeout
Description: Timeout for HTTP operations (seconds)
Type: Integer with a minimum of 0.
Default: 30

2.26.1.3.1.3renewal_via_pkcs_req
Property: VPN :: Modules :: pki :: scep :: renewal_via_pkcs_req
Description: Some SCEP servers (e.g. openxpki) are incorrectly doing certificate renewal via msgType PKCSReq (19) instead of RenewalReq (17)
Type: Boolean true or false.
Default: False

2.26.2 Profiles
Property: VPN :: Profiles
Description: IPsec-related configuration parameters from swanctl.conf
Type: JSON Object
Required: ['connections']
Default: None

2.26.2.1 CleanConf
Property: VPN :: Profiles :: CleanConf

Description: If this flag is set, the generated config files will be removed/cleaned to their default state.
Type: Boolean true or false.
Default: True

2.26.2.2 IKEStrongerThanESP
Property: VPN :: Profiles :: IKEStrongerThanESP
Type: Boolean true or false.
Description: Force IKE ciphers be stronger or equal (# of bits) than ESP ciphers.
Default: True

2.26.2.3 LocalCertificateValidation
Property: VPN :: Profiles :: LocalCertificateValidation
Type: Boolean true or false.
Description: Force the validation of preloaded certificates.
Default: True

2.26.2.4 authorities
Property: VPN :: Profiles :: authorities
Description: The list of Certificate Authorities (CAs).
Type: JSON Object
Default: None

2.26.2.4.1 authorities :: <pattern>
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$
Description: A specific CA configuration.
Type: JSON Object
Or
Required: ['cacert']
Required: ['file']
Or
Required: ['handle']
Default: None

2.26.2.4.1.1References
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: References
Description: List of other authorities sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^authorities\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.4.1.2cacert
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: cacert

Description: The CA certificate file. Only one of cacert, file, or handle may be defined for a single CA.
Type: Refer to - definitions->pki->file
Default: None

2.26.2.4.1.3file
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: file
Description: The CA certificate file. Only one of cacert, file, or handle may be defined for a single CA.
Type: Refer to - definitions->pki->file
Default: None

2.26.2.4.1.4handle
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: handle
Description: Hex-encoded CKA_ID or handle of the CA certificate on a token or TPM 2.0, respectively. Only one of cacert, file, or handle may be defined for a single CA.
Type: String pattern of ^[a-fA-F0-9]+$.
Default: None

2.26.2.4.1.5slot
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: slot
Description: Optional slot number of the token that stores the CA certificate.
Type: Integer with a minimum of 0.
Default: None

2.26.2.4.1.6module
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: module
Description: Optional PKCS#11 module name.
Type: String.
Default: None

2.26.2.4.1.7cert_uri_base
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: cert_uri_base
Description: Defines the base URI for the Hash and URL feature supported by IKEv2.
Type: Refer to - definitions->types->URI
Default: None

2.26.2.4.1.8crl_uris
Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: crl_uris
Description: A list of CRL distribution points (ldap, http, or local CRL file name).
Type: Array of unique items.
Item description: A CRL distribution point (ldap, http, or the local CRL file name).
Type: Refer to - definitions->types->URI
Default: None

2.26.2.4.1.9ocsp_uris

Property: VPN :: Profiles :: authorities :: ^[a-zA-Z0-9_-]+$ :: ocsp_uris
Description: A list of OCSP URIs.
Type: Array of unique items.
Item description: An OCSP URI.
Type: Refer to - definitions->types->URI
Default: None

2.26.2.5 Defaults
Property: VPN :: Profiles :: Defaults
Description: Sections added to define common connection or children values which can be used as references in a connection or child object.
Type: JSON Object
Default: None

2.26.2.5.1 Defaults :: <pattern>
Property: VPN :: Profiles :: Defaults :: ^[a-zA-Z0-9_-]+$
Type: Refer to - definitions->vpn->connection_base_niap
Or
Type: Refer to - definitions->vpn->children_base_niap
Default: None

2.26.2.6
connections
Property: VPN :: Profiles :: connections
Description: The list of VPN connections.
Type: JSON Object
Default: None

2.26.2.6.1 connections :: <pattern>
Property: VPN :: Profiles :: connections :: ^[a-zA-Z0-9_-]+$
Type: Refer to - definitions->vpn->connection_base_niap
Default: None

2.26.2.7 secrets
Property: VPN :: Profiles :: secrets
Description: Section defining secrets for IKE/EAP/XAuth authentication and private key decryption. The secrets section takes subsections having a specific prefix which defines the secret type. It is not recommended to define any private key decryption passphrases, as there is no real security benefit in having encrypted keys. Either store the key unencrypted or enter the keys manually when loading credentials.
Type: JSON Object
Default: None

2.26.2.7.1 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^(eap|xauth)[a-zA-Z0-9_-]{0,20}$

Description: EAP/XAuth secret subsection for a specific secret. xauth is just an alias for eap; secrets under both section prefixes are used for both EAP and XAuth authentication.
Type: JSON Object
Required: ['secret']
Default: None

2.26.2.7.1.1secret
Property: VPN :: Profiles :: secrets :: ^(eap|xauth)[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the EAP/XAuth secret. The value may either be an ASCII string, a hex encoded string if it has a 0x prefix or a Base64 encoded string if it has a 0s prefix.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.1.2References
Property: VPN :: Profiles :: secrets :: ^(eap|xauth)[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.1.3 ^(eap|xauth)[a-zA-Z0-9_-]{0,20}$ :: <pattern>
Property: VPN :: Profiles :: secrets :: ^(eap|xauth)[a-zA-Z0-9_-]{0,20}$ :: ^id[a-zA-Z0-9_-]{0,20}$
Description: Identity the EAP/XAuth secret belongs to. Multiple unique identities may be specified, each having an id prefix if a secret is shared between multiple users.
Type: String.
Default: None

2.26.2.7.2 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ntlm[a-zA-Z0-9_-]{0,20}$
Description: NTLM secret subsection for a specific secret. NTLM secrets may only be used for EAP-MSCHAPv2 authentication.
Type: JSON Object
Required: ['secret']
Default: None

2.26.2.7.2.1secret
Property: VPN :: Profiles :: secrets :: ^ntlm[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the NTLM secret. The value is the NT hash of the actual secret, i.e. MD4(UTF-16LE(secret)). The resulting 16-byte value may either be given as a hex-encoded string with a 0x prefix or as a Base64-encoded string with a 0s prefix.
Or
Type: String pattern of ^0x[a-fA-F0-9]+$.
Type: String pattern of ^0s[a-zA-Z0-9+=\/]+$.
Or

Type: Refer to - definitions->pki->file
Default: None

2.26.2.7.2.2References
Property: VPN :: Profiles :: secrets :: ^ntlm[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.2.3 ^ntlm[a-zA-Z0-9_-]{0,20}$ :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ntlm[a-zA-Z0-9_-]{0,20}$ :: ^id[a-zA-Z0-9_-]{0,20}$
Description: Identity the NTLM secret belongs to. Multiple unique identities may be specified, each having an id prefix if a secret is shared between multiple users.
Type: String.
Default: None

2.26.2.7.3 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ike[a-zA-Z0-9_-]{0,20}$
Description: IKE preshared secret section for a specific secret.
Type: JSON Object
Required: ['secret']
Default: None

2.26.2.7.3.1secret
Property: VPN :: Profiles :: secrets :: ^ike[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the IKE preshared secret. The value may either be an ASCII string, a hex-encoded string if it has a 0x prefix or a Base64-encoded string if it has a 0s prefix.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.3.2References
Property: VPN :: Profiles :: secrets :: ^ike[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.3.3 ^ike[a-zA-Z0-9_-]{0,20}$ :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ike[a-zA-Z0-9_-]{0,20}$ :: ^id[a-zA-Z0-9_-]{0,20}$
Description: Identity the IKE preshared secret belongs to. Multiple unique identities may be specified, each having an id prefix if a secret is shared between multiple users.
Type: String.
Default: None

2.26.2.7.4 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ppk[a-zA-Z0-9_-]{0,20}$
Description: Postquantum Preshared Key (PPK, RFC 8784) subsection for a specific secret.
Type: JSON Object
Required: ['secret']
Default: None

2.26.2.7.4.1secret
Property: VPN :: Profiles :: secrets :: ^ppk[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or the value of the PPK. The value may either be an ASCII string, a hex-encoded string if it has a 0x prefix or a Base64-encoded string if it has a 0s prefix. Should have at least 256 bits of entropy for 128 bit security.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.4.2References
Property: VPN :: Profiles :: secrets :: ^ppk[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.4.3 ^ppk[a-zA-Z0-9_-]{0,20}$ :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ppk[a-zA-Z0-9_-]{0,20}$ :: ^id[a-zA-Z0-9_-]{0,20}$
Description: PPK identity the PPK belongs to. Multiple unique identities may be specified, each having an id prefix if a secret is shared between multiple users.
Type: String.
Default: None

2.26.2.7.5 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^private[a-zA-Z0-9_-]{0,20}$
Description: Private key decryption passphrase for a key in the private folder.
Type: JSON Object
Required: ['file']
Default: None

2.26.2.7.5.1file
Property: VPN :: Profiles :: secrets :: ^private[a-zA-Z0-9_-]{0,20}$ :: file
Description: File name in the private folder for which this passphrase should be used.
Type: Refer to - definitions->pki->file
Default: None

2.26.2.7.5.2secret
Property: VPN :: Profiles :: secrets :: ^private[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the decryption passphrase for the private key.
Type: Refer to - definitions->pki->presharedkey_or_psk

Default: None

2.26.2.7.5.3References
Property: VPN :: Profiles :: secrets :: ^private[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.6 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^rsa[a-zA-Z0-9_-]{0,20}$
Description: Private key decryption passphrase for a key in the rsa folder.
Type: JSON Object
Required: ['file']
Default: None

2.26.2.7.6.1file
Property: VPN :: Profiles :: secrets :: ^rsa[a-zA-Z0-9_-]{0,20}$ :: file
Description: File name in the rsa folder for which this passphrase should be used.
Type: Refer to - definitions->pki->file
Default: None

2.26.2.7.6.2secret
Property: VPN :: Profiles :: secrets :: ^rsa[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the decryption passphrase for the RSA key.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.6.3References
Property: VPN :: Profiles :: secrets :: ^rsa[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.7 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^ecdsa[a-zA-Z0-9_-]{0,20}$
Description: Private key decryption passphrase for a key in the ecdsa folder.
Type: JSON Object
Required: ['file']
Default: None

2.26.2.7.7.1file
Property: VPN :: Profiles :: secrets :: ^ecdsa[a-zA-Z0-9_-]{0,20}$ :: file
Description: File name in the ecdsa folder for which this passphrase should be used.

Type: Refer to - definitions->pki->file
Default: None

2.26.2.7.7.2secret
Property: VPN :: Profiles :: secrets :: ^ecdsa[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the decryption passphrase for the ECDSA key.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.7.3References
Property: VPN :: Profiles :: secrets :: ^ecdsa[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.8 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^pkcs8[a-zA-Z0-9_-]{0,20}$
Description: Private key decryption passphrase for a key in the pkcs8 folder.
Type: JSON Object
Required: ['file']
Default: None

2.26.2.7.8.1file
Property: VPN :: Profiles :: secrets :: ^pkcs8[a-zA-Z0-9_-]{0,20}$ :: file
Description: File name in the pkcs8 folder for which this passphrase should be used.
Type: Refer to - definitions->pki->file
Default: None

2.26.2.7.8.2secret
Property: VPN :: Profiles :: secrets :: ^pkcs8[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the decryption passphrase for the PKCS#8 key.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.8.3References
Property: VPN :: Profiles :: secrets :: ^pkcs8[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.9 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^pkcs12[a-zA-Z0-9_-]{0,20}$
Description: PKCS#12 decryption passphrase for a container in the pkcs12 folder.

Type: JSON Object
Required: ['file']
Default: None

2.26.2.7.9.1file
Property: VPN :: Profiles :: secrets :: ^pkcs12[a-zA-Z0-9_-]{0,20}$ :: file
Description: File name in the pkcs12 folder for which this passphrase should be used.
Type: Refer to - definitions->pki->file
Default: None

2.26.2.7.9.2secret
Property: VPN :: Profiles :: secrets :: ^pkcs12[a-zA-Z0-9_-]{0,20}$ :: secret
Description: Either the file containing or value of the decryption passphrase for the PKCS#12 container.
Type: Refer to - definitions->pki->presharedkey_or_psk
Default: None

2.26.2.7.9.3References
Property: VPN :: Profiles :: secrets :: ^pkcs12[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.7.10 secrets :: <pattern>
Property: VPN :: Profiles :: secrets :: ^token[a-zA-Z0-9_-]{0,20}$
Description: Definition for a private key that's stored on a token, a smartcard, or a TPM 2.0.
Type: JSON Object
Required: ['handle']
Default: None

2.26.2.7.10.1 handle
Property: VPN :: Profiles :: secrets :: ^token[a-zA-Z0-9_-]{0,20}$ :: handle
Description: Hex-encoded CKA_ID or handle of the private key on the token or TPM 2.0, respectively.
Type: String pattern of ^[a-fA-F0-9]+$.
Default: None

2.26.2.7.10.2 slot
Property: VPN :: Profiles :: secrets :: ^token[a-zA-Z0-9_-]{0,20}$ :: slot
Description: Optional slot number to access the token.
Type: Integer with a minimum of 0.
Default: None

2.26.2.7.10.3 module
Property: VPN :: Profiles :: secrets :: ^token[a-zA-Z0-9_-]{0,20}$ :: module

Description: Optional PKCS#11 module name to access the token.
Type: String.
Default: None

2.26.2.7.10.4 pin
Property: VPN :: Profiles :: secrets :: ^token[a-zA-Z0-9_-]{0,20}$ :: pin
Description: Optional PIN required to access the key on the token. If none is provided the user will be prompted during connection initialization.
Default: None

2.26.2.7.10.5 References
Property: VPN :: Profiles :: secrets :: ^token[a-zA-Z0-9_-]{0,20}$ :: References
Description: List of other secrets sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^secrets\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.8 pools
Property: VPN :: Profiles :: pools
Description: List of named pools which may be referenced by connections using the pools option to assign virtual IPs and other configuration attributes. Each pool must have a unique name.
Type: JSON Object
Default: None

2.26.2.8.1 pools :: <pattern>
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$
Description: Configuration of a single named pool.
Type: JSON Object
Required: ['addrs']
Default: None

2.26.2.8.1.1addrs
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: addrs
Description: Accepts a single CIDR subnet or range defining addresses allocated in pool. Pools must be unique and non-overlapping.
Type: Refer to - definitions->types->IPAddressMaskReq
Or
Type: Refer to - definitions->types->IPAddressRange
Default: None

2.26.2.8.1.2dns
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: dns
Description: List of DNS addresses.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.2.8.1.3nbns
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: nbns
Description: List of NBNS/WINS addresses.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.2.8.1.4dhcp
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: dhcp
Description: List of DHCP server addresses.
Type: Refer to - definitions->types->IPAddressArr
Default: None

2.26.2.8.1.5netmask
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: netmask
Description: Netmask of the internal network, similar to subnet but bound to the internal address.
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.2.8.1.6server
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: server
Description: Server IP address.
Type: Refer to - definitions->types->IPAddress
Default: None

2.26.2.8.1.7subnet
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: subnet
Description: The protected sub-networks that this edge-device protects (in CIDR notation: network/mask). Usually ignored in deference to local_ts.
Type: Refer to - definitions->types->IPAddressMaskReqArr
Default: None

2.26.2.8.1.8References
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: References
Description: List of other pools sections that will be inherited into this section
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^pools\.[a-zA-Z0-9_-\.]+$.
Default: None

2.26.2.8.1.9 ^[a-zA-Z0-9_-]+$ :: <pattern>
Property: VPN :: Profiles :: pools :: ^[a-zA-Z0-9_-]+$ :: ^([1-9]|[1-9][0-9]{1,3}|[12][0-9]{4}|3[01][0-9]{3}|32[0-6][0-9]{2}|327[0-5][0-9]|3276[0-7])$
Description: Numerically identified attribute.
Type: String.
Default: None

2.27 FlowRedirector

Property: FlowRedirector
Description: Configuration of the Flow Redirection module, used to redirect flows through this router to new destinations.
Type: JSON Object
Required: ['RedirectorAddress']
Default: None

2.27.1 RedirectorAddress

Property: FlowRedirector :: RedirectorAddress
Description: The address of the redirector, where signals are received from to start/stop flow redirection.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.27.2 RedirectorPort

Property: FlowRedirector :: RedirectorPort
Description: The UDP port used for communicating with the redirector.
Type: Refer to - definitions->types->Port
Default: 9975

2.28 MANTRA

Property: MANTRA
Description: Defines the parameters for Captain Signaling Protocol/HAIPE connected interfaces.
Type: JSON Object
Required: ['serverIPs', 'Enclave']
Default: None

2.28.1 CacheLocation

Property: MANTRA :: CacheLocation
Description: The location of where the cache file should be stored, including the file name.
Type: Refer to - definitions->types->File_Dir
Default: /etc/ares/.mantraCache

2.28.2 queueNumber

Property: MANTRA :: queueNumber
Description: Queue number used by IPTables to send packets to MANTRA plugin.
Type: Integer with a minimum of 1 and a maximum of 100.
Default: 5

2.28.3 serverIPs

Property: MANTRA :: serverIPs

Description: Array with CyVis Server IP addresses.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.28.4 MREPort
Property: MANTRA :: MREPort
Description: Port for starting/receiving MRE messages, used on PT and CT side. Must match MREPlugin port.
Type: Refer to - definitions->types->Port
Default: 7777

2.28.5 NetManagerPort
Property: MANTRA :: NetManagerPort
Description: Port for sending/receiving messages from the Network Manager/CyVis.
Type: Refer to - definitions->types->Port
Default: 9971

2.28.6 MessagingDSCP
Property: MANTRA :: MessagingDSCP
Description: The TOS for CAPTAIN Signaling packets, default is 0x3F, all bits set.
Type: Integer with a minimum of 2 and a maximum of 63.
Default: 63

2.28.7 KeyframeInterval
Property: MANTRA :: KeyframeInterval
Description: Number of update frames sent between each keyframe.
Type: Integer with a minimum of 0 and a maximum of 10.
Default: 2

2.28.8 DataInterval
Property: MANTRA :: DataInterval
Description: The time, in seconds, between sending data to the visualizer. (Either keyframes or updates)
Type: Integer with a minimum of 1 and a maximum of 60.
Default: 30

2.28.9 FlowExpiration
Property: MANTRA :: FlowExpiration
Description: Time in seconds before timing out flows, both sides of the HAIPE.
Type: Integer.
Default: 30

2.28.10Enclave
Property: MANTRA :: Enclave
Description: Info for PT or CT of router.
Required: ['PT']
Default: None

2.28.10.1 PT
Property: MANTRA :: Enclave :: PT
Type: JSON Object
Required: ['HAIPEInfo', 'DSCPList']
Default: None

2.28.10.1.1 PassBeforeAck
Property: MANTRA :: Enclave :: PT :: PassBeforeAck
Description: Default state for handling traffic that has not been classified yet, default state is to DROP packets.
Type: Boolean true or false.
Default: False

2.28.10.1.2 PortPassThru
Property: MANTRA :: Enclave :: PT :: PortPassThru
Description: List of ports that will NOT be used for admission control via MANTRA.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->PortRange
Default: None

2.28.10.1.3 FlowExpiration
Property: MANTRA :: Enclave :: PT :: FlowExpiration
Description: Time in seconds before timing out flows, both sides of the HAIPE.
Type: Integer.
Default: 30

2.28.10.1.4 ICMPDSCP
Property: MANTRA :: Enclave :: PT :: ICMPDSCP
Description: DSCP value used to tag ICMP messages going across the network.
Type: Integer with a minimum of 2 and a maximum of 63.
Default: 2

2.28.10.1.5 HAIPEInfo
Property: MANTRA :: Enclave :: PT :: HAIPEInfo
Description: The HAIPE Information specific to running MANTRA for the Red/PT side on this router.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: JSON Object

Required: ['Interface', 'localHAIPE', 'ID', 'RBv6Addr']
Default: None

2.28.10.1.5.1 Interface
Property: MANTRA :: Enclave :: PT :: HAIPEInfo :: Interface
Item description: The interface connected to the HAIPE.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.28.10.1.5.2 localHAIPE
Property: MANTRA :: Enclave :: PT :: HAIPEInfo :: localHAIPE
Item description: The LocalHAIPE connected to this interface.
Type: Refer to - definitions->types->DottedQuad
Default: None

2.28.10.1.5.3 ID
Property: MANTRA :: Enclave :: PT :: HAIPEInfo :: ID
Item description: MANTRA ID for this link to this HAIPE. Matched CT side of HAIPE MANTRA ID.
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.28.10.1.5.4 RBv6Addr
Property: MANTRA :: Enclave :: PT :: HAIPEInfo :: RBv6Addr
Item description: The IPv6 Address/destination that will get signaling over the HAIPE, Red sends to this address, no default.
Type: Refer to - definitions->types->IPv6Address
Default: None

2.28.10.1.6 DSCPList
Property: MANTRA :: Enclave :: PT :: DSCPList
Description: The list of valid DSCPs used for signalling across the HAIPE.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Integer with a minimum of 2 and a maximum of 62.
Or
Required: ['CT']
Default: None

2.28.10.2 CT
Property: MANTRA :: Enclave :: CT
Type: JSON Object
Required: ['HAIPEInfo']
Default: None

2.28.10.2.1 RemoteSNATAddressesInfo

Property: MANTRA :: Enclave :: CT :: RemoteSNATAddressesInfo
Description: The alternative source addresses that are valid for other HAIPE fronted routers.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: JSON Object
Required: ['HAIPESrc', 'SNATAddrAndSubnet']
Default: None

2.28.10.2.1.1 HAIPESrc
Property: MANTRA :: Enclave :: CT :: RemoteSNATAddressesInfo :: HAIPESrc
Item description: The IP that is the true initial interface of this subnet.
Type: Refer to - definitions->types->DottedQuad
Default: None

2.28.10.2.1.2 SNATAddrAndSubnet
Property: MANTRA :: Enclave :: CT :: RemoteSNATAddressesInfo :: SNATAddrAndSubnet
Item description: The alternative source addresses of this subnet.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.28.10.2.2 HAIPEInfo
Property: MANTRA :: Enclave :: CT :: HAIPEInfo
Type: Array with a minimum number of 1 item(s) that must be unique.
Description: The information specific to running MANTRA for the Black/CT side on this router.
Item type: JSON Object
Required: ['Interface', 'SNATAddrAndSubnet', 'localHAIPE', 'SessionIDStartNum', 'ID']
Default: None

2.28.10.2.2.1 TaclaneCTv6Addr
Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: TaclaneCTv6Addr
Item description: If connected to a Taclane C100, need its black side IPv6 configured address.
Type: Refer to - definitions->types->IPv6Address
Default: None

2.28.10.2.2.2 Interface
Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: Interface
Item description: The interface connected to the HAIPE.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.28.10.2.2.3 SessionIDStartNum
Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: SessionIDStartNum
Item description: The Session ID Number for the reservation. Must be unique within entire network.
Item type: Integer with a minimum of 1.
Default: None

2.28.10.2.2.4 SessionNumberRange

Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: SessionNumberRange
Item description: The Session ID Number range to make Session IDs unique throughout the whole system, default is 500.
Item type: Integer with a minimum of 10.
Default: 500

2.28.10.2.2.5 localHAIPE

Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: localHAIPE
Item description: The LocalHAIPE connected to this interface.
Type: Refer to - definitions->types->DottedQuad
Default: None

2.28.10.2.2.6 SNATAddrAndSubnet

Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: SNATAddrAndSubnet
Item description: Black side SNAT info, the source addresses and the whole subnet for SNAT addresses.
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

2.28.10.2.2.7 ID

Property: MANTRA :: Enclave :: CT :: HAIPEInfo :: ID
Item description: MANTRA ID for this link to this HAIPE. Matches PT side of HAIPE MANTRA ID.
Item type: Integer with a minimum of 1 and a maximum of 255.
Default: None

2.29 MRE

Property: MRE
Description: Configuration for the MRE plugin.
Type: JSON Object
Required: ['serverIPs']
Default: None

2.29.1 CacheLocation

Property: MRE :: CacheLocation
Description: The location of where the cache file should be stored, including the file name.
Type: Refer to - definitions->types->File_Dir
Default: /etc/ares/.mreCache

2.29.2 UDPPort

Property: MRE :: UDPPort
Description: Port for receiving UDP messages.
Type: Refer to - definitions->types->Port

Default: 7777

2.29.3 queueNum
Property: MRE :: queueNum
Description: Queue Number for capturing traffic for the MRE.
Type: Integer with a minimum of 1 and a maximum of 100.
Default: 10

2.29.4 serverIPs
Property: MRE :: serverIPs
Description: Array with CyVis Server IP addresses.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.29.5 timeout
Property: MRE :: timeout
Description: Time (in seconds) before assuming path is invalid.
Type: Integer with a minimum of 1 and a maximum of 1000.
Default: 60

2.29.6 serverMREPort
Property: MRE :: serverMREPort
Description: CyVis server port for sending and receiving messages.
Type: Refer to - definitions->types->Port
Default: 9970

2.30 RadioController

Property: RadioController
Description: Configuration for the Radio Controller Plugin, used to translate control messages from the visualizer to a specific radio.
Type: JSON Object
Required: ['ControllerAddress']
Default: None

2.30.1 ControllerAddress
Property: RadioController :: ControllerAddress
Description: The address of the controller.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.30.2 ControllerPort
Property: RadioController :: ControllerPort
Description: The UDP port used for communicating with the controller.
Type: Refer to - definitions->types->Port
Default: 9976

2.30.3 RadioLinks
Property: RadioController :: RadioLinks
Description: List of links with radios attached that need to be controllered, along with the type of radio.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item description: Each radio link has the name of a link along with the attached radio type.
Type: Refer to - definitions->radiocontroller->BaseLink
And
Or
Type: Refer to - definitions->radiocontroller->HALOLink
Default: None

2.31 Reconfiguration

Property: Reconfiguration
Description: Configuration for the In-Mission Reconfiguration plugin.
Type: JSON Object
Default: None

2.31.1 Port
Property: Reconfiguration :: Port
Description: The port to listen for reconfiguration.
Type: Refer to - definitions->types->Port
Default: 7392

2.31.2 UseMulticast
Property: Reconfiguration :: UseMulticast
Description: Flag indicating to listen to a multicast group for reconfiguration.
Type: Boolean true or false.
Default: False

2.31.3 Source
Property: Reconfiguration :: Source
Description: The source address from which reconfiguration messages must be sent by.
Type: Refer to - definitions->types->IPv4Address
Default: 0.0.0.0

2.31.4 Group
Property: Reconfiguration :: Group
Description: The multicast group to join for reconfiguration messages. This is ignored if UseMulticast is false. Defaults to 227.22.51.7 if using multicast.
Type: Refer to - definitions->types->IPv4Multicast
Default: None

2.32 Visualizer

Property: Visualizer
Description: Configuration for the Visualizer plugin.
Type: JSON Object
Required: ['Information']
Default: None

2.32.1 KeyframeInterval
Property: Visualizer :: KeyframeInterval
Description: Number of update frames sent between each keyframe.
Type: Integer with a minimum of 0 and a maximum of 10.
Default: 3

2.32.2 DataInterval
Property: Visualizer :: DataInterval
Description: The time, in seconds, between sending data to the visualizer. (Either keyframes or updates)
Type: Integer with a minimum of 1 and a maximum of 60.
Default: 5

2.32.3 Visualizers
Property: Visualizer :: Visualizers
Description: Array of visualizer addresses where data and attack messages are sent. Not required if the network supports multicast and the multicast plugin is loaded.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.32.4 DataPort
Property: Visualizer :: DataPort
Description: The port where data and attack messages are sent.
Type: Refer to - definitions->types->Port
Default: 9977

2.32.5 UpdatePort
Property: Visualizer :: UpdatePort

Description: The port where updates are received from the visualizer.
Type: Refer to - definitions->types->Port
Default: 9978

2.32.6 MulticastGroup
Property: Visualizer :: MulticastGroup
Description: The multicast group used if the network supports multicast and the multicast plugin is loaded.
Type: Refer to - definitions->types->IPv4Multicast
Default: 224.0.1.150

2.32.7 Information
Property: Visualizer :: Information
Description: The list of alert/data information this node should send to the visualizer.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->visualizer->VisualizerInformation
Default: None

2.32.8 AttackDetection
Property: Visualizer :: AttackDetection
Description: Configuration of the attack detection information plugin.
Type: JSON Object
Required: ['Port']
Default: None

2.32.8.1 Port
Property: Visualizer :: AttackDetection :: Port
Description: The port to receive spoof attack information.
Type: Refer to - definitions->types->Port
Default: 9999

2.32.9 Flows
Property: Visualizer :: Flows
Description: Configuration of the Flow information plugin.
Type: JSON Object
Default: None

2.32.9.1 Timeout
Property: Visualizer :: Flows :: Timeout
Description: Time, in seconds, without any updates before a flow is considered invalid.
Type: Integer with a minimum of 1 and a maximum of 3600.
Default: 20

2.32.9.2 RateWindowSize
Property: Visualizer :: Flows :: RateWindowSize
Description: The rolling window size, in seconds, over which flow bit rate is averaged.
Type: Integer with a minimum of 1 and a maximum of 3600.
Default: 10

2.32.10GPS
Property: Visualizer :: GPS
Description: Configuration of the GPS information plugin.
Type: JSON Object
  Or
Required: ['Source', 'LogFile']
Default: None

2.32.10.1 Source
Property: Visualizer :: GPS :: Source
Description: The source of the GPS information.
Type: String enum of file.
Default: None

2.32.10.2 LogFile
Property: Visualizer :: GPS :: LogFile
Description: The GPS log file used by the Static GPS source.
Type: Refer to - definitions->types->File_Dir
  Or
Required: ['Source', 'GPSDAddress', 'GPSDPort']
Default: None

2.32.10.3 Source
Property: Visualizer :: GPS :: Source
Description: The source of the GPS information.
Type: String enum of gpsd.
Default: None

2.32.10.4 GPSDAddress
Property: Visualizer :: GPS :: GPSDAddress
Description: The IP address of the GPSD source.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.32.10.5 GPSDPort
Property: Visualizer :: GPS :: GPSDPort
Description: The port number of the GPSD source.
Type: Refer to - definitions->types->Port

Required: ['Source', 'Lat', 'Lon', 'Alt']
Default: None

2.32.10.6 Source
Property: Visualizer :: GPS :: Source
Description: The source of the GPS information.
Type: String enum of static.
Default: None

2.32.10.7 Lat
Property: Visualizer :: GPS :: Lat
Description: The latitude of the Static GPS source.
Type: Number.
Default: None

2.32.10.8 Lon
Property: Visualizer :: GPS :: Lon
Description: The longitude of the Static GPS source.
Type: Number.
Default: None

2.32.10.9 Alt
Property: Visualizer :: GPS :: Alt
Description: The altitude of the Static GPS source.
Type: Number.
Or
Required: ['Source']
Default: None

2.32.10.10 Source
Property: Visualizer :: GPS :: Source
Description: The source of the GPS information.
Type: String enum of android.
Default: None

2.33 TSCANR

Property: TSCANR
Description: Configuration for the T-SCANR plugin. Uses ZOOM for route advertisements and WAMS DSSS resource allocation.
Type: JSON Object
Required: ['DSSS']
Default: None

2.33.1 BridgeMode
Property: TSCANR :: BridgeMode
Description: Flag indicating if T-SCANR should run in Bridge Mode instead of Router Mode. This causes T-SCANR to not advertise routes to the router and also to directly route traffic from the SATCOM network to other T-SCANR peer modems, if the destination is reachable via a peer modem's SATCOM link. This relies on static routes being configured for each T-SCANR modem to advertise over the SATCOM link.
Type: Boolean true or false.
Default: False

2.33.2 Peers
Property: TSCANR :: Peers
Description: Configuration of Peer options.
Type: JSON Object
Default: None

2.33.2.1 StaticList
Property: TSCANR :: Peers :: StaticList
Description: List of other T-SCANR WAM devices on the same ship network. These could either provide multi-hop access to a larger DSSS network, or additional up/down links for single-hop logical COI's.
Type: Array with a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddress
Default: None

2.33.2.2 DiscoveryGroup
Property: TSCANR :: Peers :: DiscoveryGroup
Description: The multicast group used for automatic peer discovery.
Type: Refer to - definitions->types->IPv4Multicast
Default: 225.1.0.101

2.33.2.3 DiscoveryPort
Property: TSCANR :: Peers :: DiscoveryPort
Description: The destination port used for automatic peer discovery.
Type: Refer to - definitions->types->UINT16
Default: 64123

2.33.2.4 DataPort
Property: TSCANR :: Peers :: DataPort
Description: The destination port used for peer data transfers.
Type: Refer to - definitions->types->UINT16
Default: 64321

2.33.3 DSSS
Property: TSCANR :: DSSS
Description: Configuration options for the DSSS network.
Type: JSON Object
Required: ['LinkName']
Default: None

2.33.3.1 LinkName
Property: TSCANR :: DSSS :: LinkName
Description: The name of the link used for routing in/out of the DSSS network. This should be a link set up with a dummy interface.
Type: Refer to - definitions->types->InterfaceName
Default: None

2.33.3.2 Mode
Property: TSCANR :: DSSS :: Mode
Description: single-hop: T-SCANR manages resource allocation to create a logical COI making all connections a single SATCOM hop, must be supported by the modem.
multi-hop: T-SCANR coordinates multiple DSSS COI connections via multiple modems on a single ship, requires no additional modem support.
Type: String enum of single-hop, multi-hop.
Default: multi-hop

2.33.3.3 HighAssurance
Property: TSCANR :: DSSS :: HighAssurance
Description: When in DRA mode, if high assurance is turned on then one channel is always left in the listener pool to maintain node status.
Type: Boolean true or false.
Default: True

2.33.3.4 DRADelay
Property: TSCANR :: DSSS :: DRADelay
Description: The minimum delay, in microseconds, before a DSSS downlink channel can be reprogrammed to a new preset. Required in Single-Hop mode.
Type: Refer to - definitions->types->UINT32
Default: None

2.33.3.5 DRAFlowTimeout
Property: TSCANR :: DSSS :: DRAFlowTimeout
Description: The time, in seconds, of not seeing traffic before a flow is timed out. Used for freeing reserved channels.
Type: Refer to - definitions->types->UINT32
Default: None

2.33.3.6 ReRequestDelay
Property: TSCANR :: DSSS :: ReRequestDelay
Description: The time, in seconds, to delay before sending another reservation request for a previously NACK'd request.
Type: Refer to - definitions->types->UINT16
Default: 20

2.33.3.7 WAMSocketPath
Property: TSCANR :: DSSS :: WAMSocketPath
Description: The path of the Unix socket to send control data packets to the WAM platform.
Type: Refer to - definitions->types->File_Dir
Default: /var/run/wam/wam.sock

2.33.3.8 TSCANRSocketPath
Property: TSCANR :: DSSS :: TSCANRSocketPath
Description: The path of the Unix socket to receive control data packets from the WAM platform.
Type: Refer to - definitions->types->File_Dir
Default: /var/run/wam/tscanr.sock

2.33.3.9 LinkDataRequestDelay
Property: TSCANR :: DSSS :: LinkDataRequestDelay
Description: The time, in seconds, between requests sent to the WAM platform for DSSS link data (bandwidth, latency, loss).
Type: Refer to - definitions->types->UINT16
Default: 30

2.33.3.10 TAPInterfaceName
Property: TSCANR :: DSSS :: TAPInterfaceName
Description: The name of the tap interface created in which processed user data packets are sent to the WAM platform. The WAM platform must use this interface to send/receive user traffic.
Type: Refer to - definitions->types->InterfaceName
Default: wamtap0

2.33.3.11 Metrics
Property: TSCANR :: DSSS :: Metrics
Description: Static metrics for the DSSS link. Setting static metrics inhibits query to the modem.
Type: JSON Object
Default: None

2.33.3.12 Bandwidth
Property: TSCANR :: DSSS :: Metrics :: Bandwidth
Description: The bandwidth, in Kbps.
Type: Refer to - definitions->types->UINT32

Default: None

2.33.3.12.1 Latency
Property: TSCANR :: DSSS :: Metrics :: Latency
Description: The latency, in milliseconds.
Type: Refer to - definitions->types->UINT32
Default: None

2.33.3.12.2 PacketLoss
Property: TSCANR :: DSSS :: Metrics :: PacketLoss
Description: The packet loss, in percentage.
Type: Refer to - definitions->types->Percentage
Default: None

2.33.4 Router
Property: TSCANR :: Router
Description: Configuration options for the local router.
Type: JSON Object
Default: None

2.33.4.1 Address
Property: TSCANR :: Router :: Address
Description: The IP address of the On-Ship router. Required in Bridge Mode so that T-SCANR can properly router traffic between peers.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.33.4.2 RouterSocketPath
Property: TSCANR :: Router :: RouterSocketPath
Description: The path of the Unix socket to send control data packets to the Router API from T-SCANR.
Type: Refer to - definitions->types->File_Dir
Default: /var/run/tscanr/router.sock

2.33.4.3 TSCANRSocketPath
Property: TSCANR :: Router :: TSCANRSocketPath
Description: The path of the Unix socket to send control data packets to T-SCANR from the Router API.
Type: Refer to - definitions->types->File_Dir
Default: /var/run/tscanr/tscanr.sock

2.33.4.4 Protocol
Property: TSCANR :: Router :: Protocol

Description: The underlying routing protocol used to learn/advertise routes in coordination with T-SCANR.
Type: String enum of ospf, bgp.
Default: ospf

2.33.4.5 OneHopMetric
Property: TSCANR :: Router :: OneHopMetric
Description: The metric value to use when advertising One-Hop routes to the router.
Type: Refer to - definitions->types->UINT32
Default: 11111

2.33.4.6 TwoHopMetric
Property: TSCANR :: Router :: TwoHopMetric
Description: The metric value to use when advertising Two-Hop routes to the router.
Type: Refer to - definitions->types->UINT32
Default: 22222

2.33.4.7 ThreeHopMetric
Property: TSCANR :: Router :: ThreeHopMetric
Description: The metric value to use when advertising Three-Hop routes to the router.
Type: Refer to - definitions->types->UINT32
Default: 33333

2.33.4.8 BGPASN
Property: TSCANR :: Router :: BGPASN
Description: The ASN of the BGP protocol we should communicate with when configured to learn/advertise routes with BGP.
Type: Refer to - definitions->types->UINT16
Default: None

2.33.4.9 StaticRoutes
Property: TSCANR :: Router :: StaticRoutes
Description: List of static routes to always advertise on the T-SCANR network. Supports ranged subnets.
Examples:
192.168.0.0/24 // A simple single subnet.
192.168.(1-100).0/24 // A ranged subnet including everything from 192.168.1.0/24 to 192.168.100.0/24.
10.(1-10).(100-200).0/24 // A ranged subnet with multiple octets.
Type: Array of unique items.
Type: Refer to - definitions->types->DottedQuadRangeMaskReq
Default: None

2.33.5 LSA
Property: TSCANR :: LSA
Description: Configuration options for the T-SCANR LSA routing protocol.
Type: JSON Object
Default: None

2.33.5.1 Threshold
Property: TSCANR :: LSA :: Threshold
Description: The threshold, in ratio percentage of user traffic to link limit, where we stop sending LSA's and rely solely on ZOOM encoding.
Type: Refer to - definitions->types->Percentage
Default: 50

2.33.5.2 Interval
Property: TSCANR :: LSA :: Interval
Description: The time, in seconds, between sending LSA's when no changes have happened. Route changes always trigger a new LSA.
Type: Refer to - definitions->types->UINT8
Default: 10

2.33.5.3 HoldOff
Property: TSCANR :: LSA :: HoldOff
Description: The time, in seconds, between sending a new LSA when multiple changes happen in a short time frame.
Type: Refer to - definitions->types->UINT8
Default: 5

2.33.5.4 Group
Property: TSCANR :: LSA :: Group
Description: The multicast group used for LSA's.
Type: Refer to - definitions->types->IPv4Multicast
Default: 225.1.0.100

2.33.5.5 Port
Property: TSCANR :: LSA :: Port
Description: The UDP port used for LSA's.
Type: Refer to - definitions->types->Port
Default: 65432

2.33.5.6 MTU
Property: TSCANR :: LSA :: MTU
Description: The maximum size of a LSA fragment
Type: Refer to - definitions->types->UINT16
Default: 1400

2.33.6 NodeExpireDelay
Property: TSCANR :: NodeExpireDelay
Description: The time, in seconds, we will wait without receiving any updates from a discovered T-SCANR node before considering them gone from the network.
Type: Refer to - definitions->types->UINT16
Default: 120

2.33.7 RouteExpireDelay
Property: TSCANR :: RouteExpireDelay
Description: The time, in seconds, we will wait without receiving any updates about a route before considering it deleted. This is necessary because we could possibly miss the deleted route signal.
Type: Refer to - definitions->types->UINT16
Default: 300

2.33.8 JoinInterval
Property: TSCANR :: JoinInterval
Description: The time, in seconds, between sending T-SCANR join network messages.
Type: Refer to - definitions->types->UINT16
Default: 10

2.33.9 KnownSubnetsMap
Property: TSCANR :: KnownSubnetsMap
Description: List of subnets with ID->Subnet mappings. Used for route advertisement compression. Will default to the ZOOM subnet map if not defined. If no mapping defined for either, then no compression is performed.
Type: Refer to - definitions->ZOOM->SubnetMap
Default: None

2.34 BIT

Property: BIT
Description: Configuration for the Built-In Test plugin.
Type: JSON Object
Required: ['BitSources']
Default: None

2.34.1 Port
Property: BIT :: Port
Description: The TCP port.
Type: Refer to - definitions->types->Port
Default: 13495

2.34.2 CBITInterval
Property: BIT :: CBITInterval
Description: The time, in seconds, between getting updated CBIT results.
Type: Refer to - definitions->types->UINT16
Default: 10

2.34.3 IBITTimeInfo
Property: BIT :: IBITTimeInfo
Description: Enable/disable time information from being displayed in IBIT results.
Type: Boolean true or false.
Default: True

2.34.4 BitSources
Property: BIT :: BitSources
Type: Array with a minimum number of 1 item(s) that must be unique.
Or
Type: Refer to - definitions->BitSources->OnTime
Default: None

2.35 ZOOM

Property: ZOOM
Description: Configuration for the ZOOM protocol plugin.
Type: JSON Object
Default: None

2.35.1 SubnetMap
Property: ZOOM :: SubnetMap
Description: List of subnets with ID->Subnet mappings.
Type: Refer to - definitions->ZOOM->SubnetMap
Default: None

2.35.2 UseBroadcastDest
Property: ZOOM :: UseBroadcastDest
Description: Use the MAC broadcast destination rather than translating IP->MAC.
Type: Boolean true or false.
Default: False

2.35.3 UseIPSecHeader
Property: ZOOM :: UseIPSecHeader
Description: Use the header of AH/ESP packets and map SPI values to source/destination addresses.
Type: Boolean true or false.
Default: False

2.35.4 TrackIPSecSequence

Property: ZOOM :: TrackIPSecSequence
Description: Keep track of the IPSec sequence numbers, so that the field can be utilized by ZOOM and recreated on receive. This may result in more dropped packets. Only valid if special handling for IPSec packets is enabled.
Type: Boolean true or false.
Default: False

2.35.5 MinimalIPSecSPI

Property: ZOOM :: MinimalIPSecSPI
Description: Create hashed SPI values to minimize their size, so that the leftover bits can be utilized by ZOOM. This may result in more dropped packets. Only valid if special handling for IPSec packets is enabled.
Type: Boolean true or false.
Default: False

2.35.6 UseTCPHeader

Property: ZOOM :: UseTCPHeader
Description: Use the header of TCP packets.
Type: Boolean true or false.
Default: False

2.36 ZOOMClient

Property: ZOOMClient
Description: Configuration for the ZOOM remote client plugin.
Type: JSON Object
Default: None

2.36.1 ServerPort

Property: ZOOMClient :: ServerPort
Description: The TCP port.
Type: Refer to - definitions->types->Port
Default: 9797

2.36.2 ServerAddress

Property: ZOOMClient :: ServerAddress
Type: Refer to - definitions->types->IPv4Address
Default: 0.0.0.0

2.37 DHCP

Property: DHCP
Description: Global DHCP Configuration.
Type: JSON Object
Default: None

2.37.1 IPv4

Property: DHCP :: IPv4
Description: IPv4 Configuration.
Type: JSON Object
Default: None

2.37.1.1 Enable

Property: DHCP :: IPv4 :: Enable
Description: Enable the DHCPv4 server.
Type: Boolean true or false.
Default: False

2.37.1.2 Authoritative

Property: DHCP :: IPv4 :: Authoritative
Description: Set this DHCP server as the official DHCP server for the local network.
Type: Boolean true or false.
Default: False

2.37.1.3 ValidLifetime

Property: DHCP :: IPv4 :: ValidLifetime
Description: The default lease time in seconds used if the client does not request a specific lease. Default to one hour.
Type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 3600

2.37.1.4 MaxValidLifetime

Property: DHCP :: IPv4 :: MaxValidLifetime
Description: The longest lease time the server can allocate. Default to one day.
Type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 86400

2.37.1.5 OptionData

Property: DHCP :: IPv4 :: OptionData
Description: Standard DHCPv4 options; options specified at the global level apply to all subnets.
Type: Refer to - definitions->dhcp->OptionData4
Default: None

2.37.2 IPv6
Property: DHCP :: IPv6
Description: IPv6 Configuration.
Type: JSON Object
Default: None

2.37.2.1 Enable
Property: DHCP :: IPv6 :: Enable
Description: Enable the DHCPv6 server.
Type: Boolean true or false.
Default: False

2.37.2.2 ValidLifetime
Property: DHCP :: IPv6 :: ValidLifetime
Description: The default lease time in seconds used if the client does not request a specific lease. Default to one hour.
Type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 3600

2.37.2.3 MaxValidLifetime
Property: DHCP :: IPv6 :: MaxValidLifetime
Description: The longest lease time the server can allocate. Default to one day.
Type: Integer with a minimum of 60 and a maximum of 31536000.
Default: 86400

2.37.2.4 OptionData
Property: DHCP :: IPv6 :: OptionData
Description: Standard DHCPv6 options; options specified at the global level apply to all subnets.
Type: Refer to - definitions->dhcp->OptionData6
Default: None

2.38 DNS
Property: DNS
Description: DNS resolver configuration file.
Type: JSON Object
Default: None

2.38.1 Search
Property: DNS :: Search
Description: Search list for host-name lookup. By default, the search list contains one entry, the local domain name.
Type: Array with a minimum number of 1 item(s).
Item type: String.

Default: None

2.38.2 NameServers

Property: DNS :: NameServers
Description: A list of IPv4 and/or IPv6 addresses of name servers that the resolver should query. If no nameserver entries are present, the default is to use the name server on the local machine.
Type: Array with a minimum number of 1 item(s) and a maximum number of 3 item(s).
Type: Refer to - definitions->types->IPAddress
Default: None

2.38.3 Rotate

Property: DNS :: Rotate
Description: Causes round-robin selection of name servers from among those listed. This has the effect of spreading the query load among all listed servers, rather than having all clients try the first listed server first every time.
Type: Boolean true or false.
Default: False

2.38.4 Use-vc

Property: DNS :: Use-vc
Description: This option forces the use of TCP for DNS resolutions.
Type: Boolean true or false.
Default: False

2.38.5 Timeout

Property: DNS :: Timeout
Description: Sets the amount of time in seconds the resolver will wait for a response from a remote name server before retrying the query via a different name server.
Type: Integer with a minimum of 0 and a maximum of 30.
Default: 5

2.38.6 Attempts

Property: DNS :: Attempts
Description: Sets the number of times the resolver will send a query to its name servers before giving up and returning an error to the calling application
Type: Integer with a minimum of 1 and a maximum of 5.
Default: 2

2.39 NTP

Property: NTP
Description: NTP configuration
Type: JSON Object
Default: None

2.39.1 Keys

Property: NTP :: Keys
Description: An unordered list of NTP keys.
Type: Array of unique items and a maximum number of 9 item(s).
Item description: Configuration of a single NTP key.
Item type: JSON Object
Required: ['ID', 'Type', 'Key']
Default: None

2.39.1.1 ID

Property: NTP :: Keys :: ID
Item description: The key ID (1-9) to set for this key. Key IDs set here correspond to those used in the source list. Duplicate key IDs are not permitted.
Item type: Integer with a minimum of 1 and a maximum of 9.
Default: None

2.39.1.2 Type

Property: NTP :: Keys :: Type
Item description: The message digest or cipher algorithm used for this NTP key.
Item type: Enum of md5, sha1, ripemd160, sha224, sha256, sha384, sha512, aes-128, aes-192, aes-256.
Default: None

2.39.1.3 Key

Property: NTP :: Keys :: Key
Item description: Either the file containing or ASCII or hex-encoded value of the secret used as an NTP key. If used as the ControlKey, it is generally appropriate to specify the key in human-readable ASCII format. ASCII strings may be up to 20 characters in length, while hex-encoded strings may be up to 40 characters. Spaces and # characters are terminating characters and as such are not permitted.
Type: Refer to - definitions->pki->file
Or
Item type: String pattern of ^(([!"$-~](?!\.(wpa2|psk|pass))){0,20}|[0-9a-f]{0,40})$.
Default: None

2.39.2 ControlKey

Property: NTP :: ControlKey
Description: The key ID of the trusted key to be used for authentication when accessing NTP server variables (some "show ntp" commands).
Type: Integer with a minimum of 1 and a maximum of 9.
Default: None

2.39.3 Sources
Property: NTP :: Sources
Description: An ordered list of NTP sources.
Type: Array of unique items.
Item description: The configuration of a single NTP source.
Item type: JSON Object
Required: ['Address']
Default: None

2.39.3.1 Type
Property: NTP :: Sources :: Type
Item description: Set the source to server or peer type. If set to server type, time updates only flow one way: from the remote server. For peers, time updates can be exchanged in both directions.
Item type: String enum of peer, server.
Default: peer

2.39.3.2 Address
Property: NTP :: Sources :: Address
Item description: The IP address or hostname of the remote NTP server.
Type: Refer to - definitions->types->IPv4Address
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.39.3.3 KeyID
Property: NTP :: Sources :: KeyID
Item description: The key ID (1-9) of the key to be used with this peer.
Item type: Integer with a minimum of 1 and a maximum of 9.
Default: None

2.39.3.4 Prefer
Property: NTP :: Sources :: Prefer
Item description: Prefer this source. If set for multiple sources, they are preferred in the order listed.
Item type: Boolean true or false.
Default: False

2.40 Switch

Property: Switch
Description: Switch IPv4 Address
Type: JSON Object
Default: None

2.40.1 Address
Property: Switch :: Address
Description: The IP address of the switch.
Type: Refer to - definitions->types->IPv4Address
Default: None

2.41 Sysctl

Property: Sysctl
Description: Sysctl configuration; used to modify kernel parameters at runtime.
Type: JSON Object
Default: None

2.41.1 Net
Property: Sysctl :: Net
Description: Network-related kernel parameters.
Type: JSON Object
Default: None

2.41.1.1 Core
Property: Sysctl :: Net :: Core
Description: Core network parameters.
Type: JSON Object
Default: None

2.41.1.1.1 BpfJitEnable
Property: Sysctl :: Net :: Core :: BpfJitEnable
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

2.41.1.1.2 BpfJitHarden
Property: Sysctl :: Net :: Core :: BpfJitHarden
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

2.41.1.1.3 BpfJitLimit
Property: Sysctl :: Net :: Core :: BpfJitLimit
Type: Integer with a minimum of 0.
Default: 264241152

2.41.1.1.4 BusyPoll
Property: Sysctl :: Net :: Core :: BusyPoll

Type: Integer with a minimum of 0.
Default: 0

2.41.1.1.5 BusyRead
Property: Sysctl :: Net :: Core :: BusyRead
Type: Integer with a minimum of 0.
Default: 0

2.41.1.1.6 DefaultQdisc
Property: Sysctl :: Net :: Core :: DefaultQdisc
Type: String enum of choke, codel, bfifo, pfifo, fq, fq_codel, fq_pie, gred, hhf, ingress, mqprio, multiq, netem, pfifo_fast, pie, red, rr, sfb, sfq, tbf.
Default: pfifo_fast

2.41.1.1.7 DevWeight
Property: Sysctl :: Net :: Core :: DevWeight
Type: Integer.
Default: 64

2.41.1.1.8 FlowLimitCpuBitmap
Property: Sysctl :: Net :: Core :: FlowLimitCpuBitmap
Type: Integer.
Default: 0

2.41.1.1.9 FlowLimitTableLen
Property: Sysctl :: Net :: Core :: FlowLimitTableLen
Type: Integer.
Default: 4096

2.41.1.1.10 MaxSkbFrags
Property: Sysctl :: Net :: Core :: MaxSkbFrags
Type: Integer.
Default: 17

2.41.1.1.11 MessageBurst
Property: Sysctl :: Net :: Core :: MessageBurst
Type: Integer.
Default: 10

2.41.1.1.12 MessageCost
Property: Sysctl :: Net :: Core :: MessageCost
Type: Integer.
Default: 5

2.41.1.1.13 NetdevBudget
Property: Sysctl :: Net :: Core :: NetdevBudget
Type: Integer.
Default: 300

2.41.1.1.14 NetdevMaxBacklog
Property: Sysctl :: Net :: Core :: NetdevMaxBacklog
Type: Integer.
Default: 1000

2.41.1.1.15 NetdevTstampPrequeue
Property: Sysctl :: Net :: Core :: NetdevTstampPrequeue
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.1.16 OptmemMax
Property: Sysctl :: Net :: Core :: OptmemMax
Type: Integer.
Default: 20480

2.41.1.1.17 RmemDefault
Property: Sysctl :: Net :: Core :: RmemDefault
Type: Integer.
Default: 212992

2.41.1.1.18 RmemMax
Property: Sysctl :: Net :: Core :: RmemMax
Type: Integer.
Default: 212992

2.41.1.1.19 RpsSockFlowEntries
Property: Sysctl :: Net :: Core :: RpsSockFlowEntries
Type: Integer.
Default: 0

2.41.1.1.20 Somaxconn
Property: Sysctl :: Net :: Core :: Somaxconn
Type: Integer.
Default: 128

2.41.1.1.21 TstampAllowData

Property: Sysctl :: Net :: Core :: TstampAllowData
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.1.22 WmemDefault
Property: Sysctl :: Net :: Core :: WmemDefault
Type: Integer.
Default: 212992

2.41.1.1.23 WmemMax
Property: Sysctl :: Net :: Core :: WmemMax
Type: Integer.
Default: 212992

2.41.1.1.24 XfrmAcqExpires
Property: Sysctl :: Net :: Core :: XfrmAcqExpires
Type: Integer.
Default: 165

2.41.1.1.25 XfrmAeventEtime
Property: Sysctl :: Net :: Core :: XfrmAeventEtime
Type: Integer.
Default: 10

2.41.1.1.26 XfrmAeventRseqth
Property: Sysctl :: Net :: Core :: XfrmAeventRseqth
Type: Integer.
Default: 2

2.41.1.1.27 XfrmLarvalDrop
Property: Sysctl :: Net :: Core :: XfrmLarvalDrop
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2 IPv4
Property: Sysctl :: Net :: IPv4
Description: IPv4 parameters.
Type: JSON Object
Default: None

2.41.1.2.1 Conf
Property: Sysctl :: Net :: IPv4 :: Conf
Description: IPv4 configuration parameters. Parameters set here apply to all interfaces.

Type: Refer to - definitions->Sysctl->Net->IPv4->Conf
Default: None

2.41.1.2.2 Neigh
Property: Sysctl :: Net :: IPv4 :: Neigh
Description: Default IPv4 neighbor parameters.
Type: Refer to - definitions->Sysctl->Net->Neigh
Default: None

2.41.1.2.3 Route
Property: Sysctl :: Net :: IPv4 :: Route
Description: IPv4 route parameters.
Type: JSON Object
Default: None

2.41.1.2.3.1ErrorBurst
Property: Sysctl :: Net :: IPv4 :: Route :: ErrorBurst
Type: Integer.
Default: 1250

2.41.1.2.3.2ErrorCost
Property: Sysctl :: Net :: IPv4 :: Route :: ErrorCost
Type: Integer.
Default: 250

2.41.1.2.3.3GcElasticity
Property: Sysctl :: Net :: IPv4 :: Route :: GcElasticity
Type: Integer.
Default: 8

2.41.1.2.3.4GcInterval
Property: Sysctl :: Net :: IPv4 :: Route :: GcInterval
Type: Integer.
Default: 60

2.41.1.2.3.5GcMinInterval
Property: Sysctl :: Net :: IPv4 :: Route :: GcMinInterval
Type: Integer.
Default: 0

2.41.1.2.3.6GcMinIntervalMs
Property: Sysctl :: Net :: IPv4 :: Route :: GcMinIntervalMs
Type: Integer.
Default: 500

2.41.1.2.3.7GcThresh
Property: Sysctl :: Net :: IPv4 :: Route :: GcThresh
Type: Integer.
Default: -1

2.41.1.2.3.8GcTimeout
Property: Sysctl :: Net :: IPv4 :: Route :: GcTimeout
Type: Integer.
Default: 300

2.41.1.2.3.9MaxSize
Property: Sysctl :: Net :: IPv4 :: Route :: MaxSize
Type: Integer.
Default: 2147483647

2.41.1.2.3.10 MinAdvMss
Property: Sysctl :: Net :: IPv4 :: Route :: MinAdvMss
Type: Integer.
Default: 256

2.41.1.2.3.11 MinPmtu
Property: Sysctl :: Net :: IPv4 :: Route :: MinPmtu
Type: Integer.
Default: 552

2.41.1.2.3.12 MtuExpires
Property: Sysctl :: Net :: IPv4 :: Route :: MtuExpires
Type: Integer.
Default: 600

2.41.1.2.3.13 RedirectLoad
Property: Sysctl :: Net :: IPv4 :: Route :: RedirectLoad
Type: Integer.
Default: 5

2.41.1.2.3.14 RedirectNumber
Property: Sysctl :: Net :: IPv4 :: Route :: RedirectNumber
Type: Integer.
Default: 9

2.41.1.2.3.15 RedirectSilence
Property: Sysctl :: Net :: IPv4 :: Route :: RedirectSilence
Type: Integer.
Default: 5120

2.41.1.2.3.16 Misc

Property: Sysctl :: Net :: IPv4 :: Misc
Description: Misc IPv4 parameters.
Type: JSON Object
Default: None

2.41.1.2.3.17 FibMultipathUseNeigh
Property: Sysctl :: Net :: IPv4 :: Misc :: FibMultipathUseNeigh
Description: Use status of existing neighbor entry when determining nexthop for multipath routes. If disabled, neighbor information is not used and packets could be directed to a failed nexthop. Only valid for kernels built with CONFIG_IP_ROUTE_MULTIPATH enabled. 0 - disabled. 1 - enabled.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.18 FwmarkReflect
Property: Sysctl :: Net :: IPv4 :: Misc :: FwmarkReflect
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.19 IcmpEchoIgnoreAll
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpEchoIgnoreAll
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.20 IcmpEchoIgnoreBroadcasts
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpEchoIgnoreBroadcasts
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.21 IcmpErrorsUseInboundIfaddr
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpErrorsUseInboundIfaddr
Description: 0 - ICMP error messages are sent with the primary address of the exiting interface. 1 - the message will be sent with the primary address of the interface that received the packet that caused the ICMP error. This is the behaviour many network administrators will expect from a router. And it can make debugging complicated network layouts much easier. Note that if no primary address exists for the interface selected, then the primary address of the first non-loopback interface that has one will be used regardless of this setting.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.22 IcmpIgnoreBogusErrorResponses
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpIgnoreBogusErrorResponses
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.23 IcmpMsgsBurst

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpMsgsBurst
Type: Integer.
Default: 50

2.41.1.2.3.24 IcmpMsgsPerSec
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpMsgsPerSec
Type: Integer.
Default: 1000

2.41.1.2.3.25 IcmpRatelimit
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpRatelimit
Type: Integer.
Default: 1000

2.41.1.2.3.26 IcmpRatemask
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpRatemask
Type: Integer.
Default: 6168

2.41.1.2.3.27 IgmpLinkLocalMcastReports
Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpLinkLocalMcastReports
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.28 IgmpMaxMemberships
Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpMaxMemberships
Description: Change the maximum number of multicast groups we can subscribe to.
Type: Integer with a minimum of 0 and a maximum of 5459.
Default: 1000

2.41.1.2.3.29 IgmpMaxMsf
Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpMaxMsf
Type: Integer.
Default: 10

2.41.1.2.3.30 IgmpQrv
Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpQrv
Type: Integer with a minimum of 1.
Default: 2

2.41.1.2.3.31 InetPeerMaxttl
Property: Sysctl :: Net :: IPv4 :: Misc :: InetPeerMaxttl
Type: Integer with a minimum of 0.
Default: 600

2.41.1.2.3.32 InetPeerMinttl

Property: Sysctl :: Net :: IPv4 :: Misc :: InetPeerMinttl
Type: Integer with a minimum of 0.
Default: 120

2.41.1.2.3.33 InetPeerThreshold
Property: Sysctl :: Net :: IPv4 :: Misc :: InetPeerThreshold
Type: Integer.
Default: 65664

2.41.1.2.3.34 IpDefaultTtl
Property: Sysctl :: Net :: IPv4 :: Misc :: IpDefaultTtl
Type: Integer.
Default: 64

2.41.1.2.3.35 IpDynaddr
Property: Sysctl :: Net :: IPv4 :: Misc :: IpDynaddr
Type: Integer with a minimum of 0.
Default: 0

2.41.1.2.3.36 IpEarlyDemux
Property: Sysctl :: Net :: IPv4 :: Misc :: IpEarlyDemux
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.37 IpForward
Property: Sysctl :: Net :: IPv4 :: Misc :: IpForward
Description: Forward packets between interfaces.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.38 IpForwardUsePmtu
Property: Sysctl :: Net :: IPv4 :: Misc :: IpForwardUsePmtu
Description: Trust protocol path MTUs while forwarding packets.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.39 IpLocalPortRange
Property: Sysctl :: Net :: IPv4 :: Misc :: IpLocalPortRange
Type: Array with a minimum number of 2 item(s) and a maximum number of 2 item(s).
Item type: Integer with a minimum of 1 and a maximum of 65535.
Default: None

2.41.1.2.3.40 IpLocalReservedPorts
Property: Sysctl :: Net :: IPv4 :: Misc :: IpLocalReservedPorts
Type: Array.
Type: Refer to - definitions->types->PortRange

Default: None

2.41.1.2.3.41 IpNoPmtuDisc
Property: Sysctl :: Net :: IPv4 :: Misc :: IpNoPmtuDisc
Type: Integer with a minimum of 0 and a maximum of 3.
Default: 0

2.41.1.2.3.42 IpNonlocalBind
Property: Sysctl :: Net :: IPv4 :: Misc :: IpNonlocalBind
Description: If set, allows processes to bind to non-local IP addresses, which can be quite useful - but may break some applications.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.43 IpfragHighThresh
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragHighThresh
Type: Integer.
Default: 4194304

2.41.1.2.3.44 IpfragLowThresh
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragLowThresh
Type: Integer.
Default: 3145728

2.41.1.2.3.45 IpfragMaxDist
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragMaxDist
Type: Integer with a minimum of 0.
Default: 64

2.41.1.2.3.46 IpfragSecretInterval
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragSecretInterval
Type: Integer with a minimum of 0.
Default: 0

2.41.1.2.3.47 IpfragTime
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragTime
Type: Integer with a minimum of 0.
Default: 30

2.41.1.2.3.48 PingGroupRange
Property: Sysctl :: Net :: IPv4 :: Misc :: PingGroupRange
Type: Array with a minimum number of 2 item(s) and a maximum number of 2 item(s).
Type: Refer to - definitions->types->UINT32
Default: None

2.41.1.2.3.49 TcpAbortOnOverflow

Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAbortOnOverflow
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.50 TcpAdvWinScale
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAdvWinScale
Type: Integer with a minimum of -31 and a maximum of 31.
Default: 1

2.41.1.2.3.51 TcpAllowedCongestionControl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAllowedCongestionControl
Type: String.
Default: cubic reno

2.41.1.2.3.52 TcpAppWin
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAppWin
Type: Integer.
Default: 31

2.41.1.2.3.53 TcpAutocorking
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAutocorking
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.54 TcpAvailableCongestionControl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAvailableCongestionControl
Type: String.
Default: cubic reno

2.41.1.2.3.55 TcpBaseMss
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpBaseMss
Type: Integer.
Default: 1024

2.41.1.2.3.56 TcpChallengeAckLimit
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpChallengeAckLimit
Type: Integer.
Default: 1000

2.41.1.2.3.57 TcpCongestionControl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpCongestionControl
Type: String.
Default: cubic

2.41.1.2.3.58 TcpDsack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpDsack

Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.59 TcpEarlyRetrans
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpEarlyRetrans
Type: Integer enum of 0, 3, 4.
Default: 3

2.41.1.2.3.60 TcpEcn
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpEcn
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 2

2.41.1.2.3.61 TcpEcnFallback
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpEcnFallback
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.62 TcpFack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFack
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.63 TcpFastopen
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFastopen
Type: Integer.
Default: 1

2.41.1.2.3.64 TcpFastopenKey
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFastopenKey
Type: Array with a minimum number of 1 item(s) and a maximum number of 2 item(s).
Item type: String with a maximum length of 35 and a pattern of ^[a-fA-F0-9]{1,8}(-[a-fA-F0-9]{1,8}){3}$.
Default: None

2.41.1.2.3.65 TcpFinTimeout
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFinTimeout
Type: Integer with a minimum of 0.
Default: 60

2.41.1.2.3.66 TcpFrto
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFrto
Type: Integer.
Default: 2

2.41.1.2.3.67 TcpFwmarkAccept

Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFwmarkAccept
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.68 TcpInvalidRatelimit
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpInvalidRatelimit
Type: Integer.
Default: 500

2.41.1.2.3.69 TcpKeepaliveIntvl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpKeepaliveIntvl
Type: Integer.
Default: 75

2.41.1.2.3.70 TcpKeepaliveProbes
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpKeepaliveProbes
Type: Integer.
Default: 9

2.41.1.2.3.71 TcpKeepaliveTime
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpKeepaliveTime
Type: Integer.
Default: 7200

2.41.1.2.3.72 TcpL3mdevAccept
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpL3mdevAccept
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.73 TcpLimitOutputBytes
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpLimitOutputBytes
Type: Integer.
Default: 262144

2.41.1.2.3.74 TcpMaxOrphans
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxOrphans
Type: Integer.
Default: 32768

2.41.1.2.3.75 TcpMaxReordering
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxReordering
Type: Integer.
Default: 300

2.41.1.2.3.76 TcpMaxSynBacklog
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxSynBacklog

Type: Integer with a minimum of 128.
Default: 256

2.41.1.2.3.77 TcpMaxTwBuckets
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxTwBuckets
Type: Integer.
Default: 32768

2.41.1.2.3.78 TcpMem
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.2.3.79 TcpMinRttWlen
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMinRttWlen
Type: Integer with a minimum of 0 and a maximum of 86400.
Default: 300

2.41.1.2.3.80 TcpMinSndMss
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMinSndMss
Type: Integer.
Default: 48

2.41.1.2.3.81 TcpMinTsoSegs
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMinTsoSegs
Type: Integer.
Default: 2

2.41.1.2.3.82 TcpModerateRcvbuf
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpModerateRcvbuf
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.83 TcpMtuProbing
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMtuProbing
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0
2.41.1.2.3.84
TcpNoMetricsSave
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpNoMetricsSave
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.85 TcpNotsentLowat
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpNotsentLowat

Type: Integer.
Default: 4294967295

2.41.1.2.3.86 TcpOrphanRetries
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpOrphanRetries
Type: Integer.
Default: 0

2.41.1.2.3.87 TcpPacingCaRatio
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpPacingCaRatio
Type: Integer.
Default: 120

2.41.1.2.3.88 TcpPacingSsRatio
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpPacingSsRatio
Type: Integer.
Default: 200

2.41.1.2.3.89 TcpProbeInterval
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpProbeInterval
Type: Integer.
Default: 600

2.41.1.2.3.90 TcpProbeThreshold
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpProbeThreshold
Type: Integer.
Default: 8

2.41.1.2.3.91 TcpRecovery
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRecovery
Type: Integer.
Default: 1

2.41.1.2.3.92 TcpReordering
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpReordering
Type: Integer.
Default: 3

2.41.1.2.3.93 TcpRetransCollapse
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRetransCollapse
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.94 TcpRetries1
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRetries1
Type: Integer.

Default: 3

2.41.1.2.3.95 TcpRetries2
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRetries2
Type: Integer.
Default: 15

2.41.1.2.3.96 TcpRfc1337
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRfc1337
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.97 TcpRmem
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRmem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.2.3.98 TcpSack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSack
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.99 TcpSlowStartAfterIdle
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSlowStartAfterIdle
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.100 TcpStdurg
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpStdurg
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.101 TcpSynRetries
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSynRetries
Type: Integer with a minimum of 0 and a maximum of 127.
Default: 6

2.41.1.2.3.102 TcpSynackRetries
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSynackRetries
Type: Integer with a minimum of 0 and a maximum of 255.
Default: 5

2.41.1.2.3.103 TcpSyncookies
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSyncookies
Type: Integer.

Default: 1

2.41.1.2.3.104 TcpThinDupack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpThinDupack
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.105 TcpThinLinearTimeouts
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpThinLinearTimeouts
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.106 TcpTimestamps
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpTimestamps
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 1

2.41.1.2.3.107 TcpTsoWinDivisor
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpTsoWinDivisor
Type: Integer.
Default: 3

2.41.1.2.3.108 TcpTwReuse
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpTwReuse
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

2.41.1.2.3.109 TcpWindowScaling
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpWindowScaling
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.2.3.110 TcpWmem
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpWmem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.2.3.111 TcpWorkaroundSignedWindows
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpWorkaroundSignedWindows
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.2.3.112 UdpMem
Property: Sysctl :: Net :: IPv4 :: Misc :: UdpMem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).

Item type: Integer.
Default: None

2.41.1.2.3.113 UdpRmemMin
Property: Sysctl :: Net :: IPv4 :: Misc :: UdpRmemMin
Type: Integer.
Default: 4096

2.41.1.2.3.114 UdpWmemMin
Property: Sysctl :: Net :: IPv4 :: Misc :: UdpWmemMin
Type: Integer.
Default: 4096

2.41.1.2.3.115 Xfrm4GcThresh
Property: Sysctl :: Net :: IPv4 :: Misc :: Xfrm4GcThresh
Type: Integer.
Default: 2147483647

2.41.1.3 IPv6
Property: Sysctl :: Net :: IPv6
Description: IPv6 parameters.
Type: JSON Object
Default: None

2.41.1.3.1 Conf
Property: Sysctl :: Net :: IPv6 :: Conf
Description: IPv6 configuration parameters. Parameters set here apply to all interfaces.
Type: Refer to - definitions->Sysctl->Net->IPv6->Conf
Default: None

2.41.1.3.2 Neigh
Property: Sysctl :: Net :: IPv6 :: Neigh
Description: Default IPv6 neighbor parameters.
Type: Refer to - definitions->Sysctl->Net->Neigh
Default: None

2.41.1.3.3 Route
Property: Sysctl :: Net :: IPv6 :: Route
Description: IPv6 route parameters.
Type: JSON Object
Default: None

2.41.1.3.3.1GcElasticity
Property: Sysctl :: Net :: IPv6 :: Route :: GcElasticity

Type: Integer.
Default: 9

2.41.1.3.3.2GcInterval
Property: Sysctl :: Net :: IPv6 :: Route :: GcInterval
Type: Integer.
Default: 30

2.41.1.4 GcMinInterval
Property: Sysctl :: Net :: IPv6
Type: Integer.
Default: 0

2.41.1.4.1 GcMinIntervalMs
Property: Sysctl :: Net :: IPv4 :: Route :: GcMinIntervalMs
Type: Integer.
Default: 500

2.41.1.4.1.1GcThresh
Property: Sysctl :: Net :: IPv4 :: Route :: GcThresh
Type: Integer.
Default: -1

2.41.1.4.1.2GcTimeout
Property: Sysctl :: Net :: IPv4 :: Route :: GcTimeout
Type: Integer.
Default: 300

2.41.1.4.1.3MaxSize
Property: Sysctl :: Net :: IPv4 :: Route :: MaxSize
Type: Integer.
Default: 2147483647

2.41.1.4.1.4MinAdvMss
Property: Sysctl :: Net :: IPv4 :: Route :: MinAdvMss
Type: Integer.
Default: 256

2.41.1.4.1.5MinPmtu
Property: Sysctl :: Net :: IPv4 :: Route :: MinPmtu
Type: Integer.
Default: 552

2.41.1.4.1.6MtuExpires
Property: Sysctl :: Net :: IPv4 :: Route :: MtuExpires

Type: Integer.
Default: 600

2.41.1.4.1.7 RedirectLoad
Property: Sysctl :: Net :: IPv4 :: Route :: RedirectLoad
Type: Integer.
Default: 5

2.41.1.4.1.8 RedirectNumber
Property: Sysctl :: Net :: IPv4 :: Route :: RedirectNumber
Type: Integer.
Default: 9

2.41.1.4.1.9 RedirectSilence
Property: Sysctl :: Net :: IPv4 :: Route :: RedirectSilence
Type: Integer.
Default: 5120

2.41.1.4.1.10 Misc
Property: Sysctl :: Net :: IPv4 :: Misc
Description: Misc IPv4 parameters.
Type: JSON Object
Default: None

2.41.1.4.1.11 FibMultipathUseNeigh
Property: Sysctl :: Net :: IPv4 :: Misc :: FibMultipathUseNeigh
Description: Use status of existing neighbor entry when determining nexthop for multipath routes. If disabled, neighbor information is not used and packets could be directed to a failed nexthop. Only valid for kernels built with CONFIG_IP_ROUTE_MULTIPATH enabled. 0 - disabled. 1 - enabled.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.12 FwmarkReflect
Property: Sysctl :: Net :: IPv4 :: Misc :: FwmarkReflect
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.13 IcmpEchoIgnoreAll
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpEchoIgnoreAll
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.14 IcmpEchoIgnoreBroadcasts
Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpEchoIgnoreBroadcasts
Type: Refer to - definitions->types->BooleanInt

Default: 1

2.41.1.4.1.15 IcmpErrorsUseInboundIfaddr

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpErrorsUseInboundIfaddr
Description: 0 - ICMP error messages are sent with the primary address of the exiting interface. 1 - the message will be sent with the primary address of the interface that received the packet that caused the ICMP error. This is the behaviour many network administrators will expect from a router. And it can make debugging complicated network layouts much easier. Note that if no primary address exists for the interface selected, then the primary address of the first non-loopback interface that has one will be used regardless of this setting.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.16 IcmpIgnoreBogusErrorResponses

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpIgnoreBogusErrorResponses
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.17 IcmpMsgsBurst

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpMsgsBurst
Type: Integer.
Default: 50

2.41.1.4.1.18 IcmpMsgsPerSec

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpMsgsPerSec
Type: Integer.
Default: 1000

2.41.1.4.1.19 IcmpRatelimit

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpRatelimit
Type: Integer.
Default: 1000

2.41.1.4.1.20 IcmpRatemask

Property: Sysctl :: Net :: IPv4 :: Misc :: IcmpRatemask
Type: Integer.
Default: 6168

2.41.1.4.1.21 IgmpLinkLocalMcastReports

Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpLinkLocalMcastReports
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.22 IgmpMaxMemberships

Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpMaxMemberships
Description: Change the maximum number of multicast groups we can subscribe to.

Type: Integer with a minimum of 0 and a maximum of 5459.
Default: 1000

2.41.1.4.1.23 IgmpMaxMsf
Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpMaxMsf
Type: Integer.
Default: 10

2.41.1.4.1.24 IgmpQrv
Property: Sysctl :: Net :: IPv4 :: Misc :: IgmpQrv
Type: Integer with a minimum of 1.
Default: 2

2.41.1.4.1.25 InetPeerMaxttl
Property: Sysctl :: Net :: IPv4 :: Misc :: InetPeerMaxttl
Type: Integer with a minimum of 0.
Default: 600

2.41.1.4.1.26 InetPeerMinttl
Property: Sysctl :: Net :: IPv4 :: Misc :: InetPeerMinttl
Type: Integer with a minimum of 0.
Default: 120

2.41.1.4.1.27 InetPeerThreshold
Property: Sysctl :: Net :: IPv4 :: Misc :: InetPeerThreshold
Type: Integer.
Default: 65664

2.41.1.4.1.28 IpDefaultTtl
Property: Sysctl :: Net :: IPv4 :: Misc :: IpDefaultTtl
Type: Integer.
Default: 64

2.41.1.4.1.29 IpDynaddr
Property: Sysctl :: Net :: IPv4 :: Misc :: IpDynaddr
Type: Integer with a minimum of 0.
Default: 0

2.41.1.4.1.30 IpEarlyDemux
Property: Sysctl :: Net :: IPv4 :: Misc :: IpEarlyDemux
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.31 IpForward
Property: Sysctl :: Net :: IPv4 :: Misc :: IpForward
Description: Forward packets between interfaces.

Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.32 IpForwardUsePmtu
Property: Sysctl :: Net :: IPv4 :: Misc :: IpForwardUsePmtu
Description: Trust protocol path MTUs while forwarding packets.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.33 IpLocalPortRange
Property: Sysctl :: Net :: IPv4 :: Misc :: IpLocalPortRange
Type: Array with a minimum number of 2 item(s) and a maximum number of 2 item(s).
Item type: Integer with a minimum of 1 and a maximum of 65535.
Default: None

2.41.1.4.1.34 IpLocalReservedPorts
Property: Sysctl :: Net :: IPv4 :: Misc :: IpLocalReservedPorts
Type: Array.
Type: Refer to - definitions->types->PortRange
Default: None

2.41.1.4.1.35 IpNoPmtuDisc
Property: Sysctl :: Net :: IPv4 :: Misc :: IpNoPmtuDisc
Type: Integer with a minimum of 0 and a maximum of 3.
Default: 0

2.41.1.4.1.36 IpNonlocalBind
Property: Sysctl :: Net :: IPv4 :: Misc :: IpNonlocalBind
Description: If set, allows processes to bind to non-local IP addresses, which can be quite useful - but may break some applications.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.37 IpfragHighThresh
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragHighThresh
Type: Integer.
Default: 4194304

2.41.1.4.1.38 IpfragLowThresh
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragLowThresh
Type: Integer.
Default: 3145728

2.41.1.4.1.39 IpfragMaxDist
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragMaxDist
Type: Integer with a minimum of 0.

Default: 64

2.41.1.4.1.40 IpfragSecretInterval
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragSecretInterval
Type: Integer with a minimum of 0.
Default: 0

2.41.1.4.1.41 IpfragTime
Property: Sysctl :: Net :: IPv4 :: Misc :: IpfragTime
Type: Integer with a minimum of 0.
Default: 30

2.41.1.4.1.42 PingGroupRange
Property: Sysctl :: Net :: IPv4 :: Misc :: PingGroupRange
Type: Array with a minimum number of 2 item(s) and a maximum number of 2 item(s).
Type: Refer to - definitions->types->UINT32
Default: None

2.41.1.4.1.43 TcpAbortOnOverflow
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAbortOnOverflow
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.44 TcpAdvWinScale
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAdvWinScale
Type: Integer with a minimum of -31 and a maximum of 31.
Default: 1

2.41.1.4.1.45 TcpAllowedCongestionControl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAllowedCongestionControl
Type: String.
Default: cubic reno

2.41.1.4.1.46 TcpAppWin
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAppWin
Type: Integer.
Default: 31

2.41.1.4.1.47 TcpAutocorking
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAutocorking
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.48 TcpAvailableCongestionControl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpAvailableCongestionControl
Type: String.

Default: cubic reno

2.41.1.4.1.49 TcpBaseMss
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpBaseMss
Type: Integer.
Default: 1024

2.41.1.4.1.50 TcpChallengeAckLimit
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpChallengeAckLimit
Type: Integer.
Default: 1000

2.41.1.4.1.51 TcpCongestionControl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpCongestionControl
Type: String.
Default: cubic

2.41.1.4.1.52 TcpDsack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpDsack
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.53 TcpEarlyRetrans
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpEarlyRetrans
Type: Integer enum of 0, 3, 4.
Default: 3

2.41.1.4.1.54 TcpEcn
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpEcn
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 2

2.41.1.4.1.55 TcpEcnFallback
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpEcnFallback
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.56 TcpFack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFack
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.57 TcpFastopen
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFastopen
Type: Integer.
Default: 1

2.41.1.4.1.58 TcpFastopenKey
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFastopenKey
Type: Array with a minimum number of 1 item(s) and a maximum number of 2 item(s).
Item type: String with a maximum length of 35 and a pattern of ^[a-fA-F0-9]{1,8}(-[a-fA-F0-9]{1,8}){3}$.
Default: None

2.41.1.4.1.59 TcpFinTimeout
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFinTimeout
Type: Integer with a minimum of 0.
Default: 60

TcpFrto
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFrto
Type: Integer.
Default: 2

2.41.1.4.1.60 TcpFwmarkAccept
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpFwmarkAccept
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.61 TcpInvalidRatelimit
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpInvalidRatelimit
Type: Integer.
Default: 500

2.41.1.4.1.62 TcpKeepaliveIntvl
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpKeepaliveIntvl
Type: Integer.
Default: 75

2.41.1.4.1.63 TcpKeepaliveProbes
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpKeepaliveProbes
Type: Integer.
Default: 9

2.41.1.4.1.64 TcpKeepaliveTime
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpKeepaliveTime
Type: Integer.
Default: 7200

2.41.1.4.1.65 TcpL3mdevAccept
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpL3mdevAccept
Type: Refer to - definitions->types->BooleanInt

Default: 0

2.41.1.4.1.66 TcpLimitOutputBytes
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpLimitOutputBytes
Type: Integer.
Default: 262144

2.41.1.4.1.67 TcpMaxOrphans
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxOrphans
Type: Integer.
Default: 32768

2.41.1.4.1.68 TcpMaxReordering
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxReordering
Type: Integer.
Default: 300

2.41.1.4.1.69 TcpMaxSynBacklog
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxSynBacklog
Type: Integer with a minimum of 128.
Default: 256

2.41.1.4.1.70 TcpMaxTwBuckets
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMaxTwBuckets
Type: Integer.
Default: 32768

2.41.1.4.1.71 TcpMem
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.4.1.72 TcpMinRttWlen
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMinRttWlen
Type: Integer with a minimum of 0 and a maximum of 86400.
Default: 300

2.41.1.4.1.73 TcpMinSndMss
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMinSndMss
Type: Integer.
Default: 48

2.41.1.4.1.74 TcpMinTsoSegs
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMinTsoSegs
Type: Integer.

Default: 2

2.41.1.4.1.75 TcpModerateRcvbuf
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpModerateRcvbuf
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.76 TcpMtuProbing
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpMtuProbing
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

2.41.1.4.1.77 TcpNoMetricsSave
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpNoMetricsSave
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.78 TcpNotsentLowat
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpNotsentLowat
Type: Integer.
Default: 4294967295

2.41.1.4.1.79 TcpOrphanRetries
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpOrphanRetries
Type: Integer.
Default: 0

2.41.1.4.1.80 TcpPacingCaRatio
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpPacingCaRatio
Type: Integer.
Default: 120

2.41.1.4.1.81 TcpPacingSsRatio
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpPacingSsRatio
Type: Integer.
Default: 200

2.41.1.4.1.82 TcpProbeInterval
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpProbeInterval
Type: Integer.
Default: 600

2.41.1.4.1.83 TcpProbeThreshold
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpProbeThreshold
Type: Integer.
Default: 8

2.41.1.4.1.84 TcpRecovery
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRecovery
Type: Integer.
Default: 1

2.41.1.4.1.85 TcpReordering
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpReordering
Type: Integer.
Default: 3

2.41.1.4.1.86 TcpRetransCollapse
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRetransCollapse
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.87 TcpRetries1
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRetries1
Type: Integer.
Default: 3

2.41.1.4.1.88 TcpRetries2
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRetries2
Type: Integer.
Default: 15

2.41.1.4.1.89 TcpRfc1337
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRfc1337
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.90 TcpRmem
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpRmem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.4.1.91 TcpSack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSack
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.92 TcpSlowStartAfterIdle
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSlowStartAfterIdle
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.93 TcpStdurg
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpStdurg
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.94 TcpSynRetries
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSynRetries
Type: Integer with a minimum of 0 and a maximum of 127.
Default: 6

2.41.1.4.1.95 TcpSynackRetries
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSynackRetries
Type: Integer with a minimum of 0 and a maximum of 255.
Default: 5

2.41.1.4.1.96 TcpSyncookies
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpSyncookies
Type: Integer.
Default: 1

2.41.1.4.1.97 TcpThinDupack
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpThinDupack
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.98 TcpThinLinearTimeouts
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpThinLinearTimeouts
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.99 TcpTimestamps
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpTimestamps
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 1

2.41.1.4.1.100 TcpTsoWinDivisor
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpTsoWinDivisor
Type: Integer.
Default: 3

2.41.1.4.1.101 TcpTwReuse
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpTwReuse
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

2.41.1.4.1.102 TcpWindowScaling
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpWindowScaling
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.4.1.103 TcpWmem
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpWmem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.4.1.104 TcpWorkaroundSignedWindows
Property: Sysctl :: Net :: IPv4 :: Misc :: TcpWorkaroundSignedWindows
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.4.1.105 UdpMem
Property: Sysctl :: Net :: IPv4 :: Misc :: UdpMem
Type: Array with a minimum number of 3 item(s) and a maximum number of 3 item(s).
Item type: Integer.
Default: None

2.41.1.4.1.106 UdpRmemMin
Property: Sysctl :: Net :: IPv4 :: Misc :: UdpRmemMin
Type: Integer.
Default: 4096

2.41.1.4.1.107 UdpWmemMin
Property: Sysctl :: Net :: IPv4 :: Misc :: UdpWmemMin
Type: Integer.
Default: 4096

2.41.1.4.1.108 Xfrm4GcThresh
Property: Sysctl :: Net :: IPv4 :: Misc :: Xfrm4GcThresh
Type: Integer.
Default: 2147483647

2.41.1.5 IPv6
Property: Sysctl :: Net :: IPv6
Description: IPv6 parameters.
Type: JSON Object
Default: None

2.41.1.5.1 Conf
Property: Sysctl :: Net :: IPv6 :: Conf

Description: IPv6 configuration parameters. Parameters set here apply to all interfaces.
Type: Refer to - definitions->Sysctl->Net->IPv6->Conf
Default: None

2.41.1.5.2 Neigh
Property: Sysctl :: Net :: IPv6 :: Neigh
Description: Default IPv6 neighbor parameters.
Type: Refer to - definitions->Sysctl->Net->Neigh
Default: None

2.41.1.5.3 Route
Property: Sysctl :: Net :: IPv6 :: Route
Description: IPv6 route parameters.
Type: JSON Object
Default: None

2.41.1.5.3.1GcElasticity
Property: Sysctl :: Net :: IPv6 :: Route :: GcElasticity
Type: Integer.
Default: 9

2.41.1.5.3.2GcInterval
Property: Sysctl :: Net :: IPv6 :: Route :: GcInterval
Type: Integer.
Default: 30

2.41.1.5.3.3GcMinInterval
Property: Sysctl :: Net :: IPv6 :: Route :: GcMinInterval
Type: Integer.
Default: 0

2.41.1.5.3.4GcMinIntervalMs
Property: Sysctl :: Net :: IPv6 :: Route :: GcMinIntervalMs
Type: Integer.
Default: 500

2.41.1.5.3.5GcThresh
Property: Sysctl :: Net :: IPv6 :: Route :: GcThresh
Type: Integer.
Default: 1024

2.41.1.5.3.6GcTimeout
Property: Sysctl :: Net :: IPv6 :: Route :: GcTimeout
Type: Integer.
Default: 60

2.41.1.5.3.7MaxSize
Property: Sysctl :: Net :: IPv6 :: Route :: MaxSize
Type: Integer with a minimum of 0.
Default: 4096

2.41.1.5.3.8MinAdvMss
Property: Sysctl :: Net :: IPv6 :: Route :: MinAdvMss
Type: Integer.
Default: 1220

2.41.1.5.3.9MtuExpires
Property: Sysctl :: Net :: IPv6 :: Route :: MtuExpires
Type: Integer.
Default: 600

2.41.1.5.3.10 SkipNotifyOnDevDown
Property: Sysctl :: Net :: IPv6 :: Route :: SkipNotifyOnDevDown
Description: Controls whether an RTM_DELROUTE message is generated for routes removed when a device is taken down or deleted. IPv4 does not generate this message; IPv6 does by default. Setting this sysctl to true (1) skips the message, making IPv4 and IPv6 on par in relying on userspace caches to track link events and evict routes.
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.5.4 Misc
Property: Sysctl :: Net :: IPv6 :: Misc
Description: Misc IPv6 parameters.
Type: JSON Object
Default: None

2.41.1.5.4.1AnycastSrcEchoReply
Property: Sysctl :: Net :: IPv6 :: Misc :: AnycastSrcEchoReply
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.5.4.2AutoFlowlabels
Property: Sysctl :: Net :: IPv6 :: Misc :: AutoFlowlabels
Type: Integer with a minimum of 0 and a maximum of 3.
Default: 1

2.41.1.5.4.3Bindv6only
Property: Sysctl :: Net :: IPv6 :: Misc :: Bindv6only
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.5.4.4FlowlabelConsistency
Property: Sysctl :: Net :: IPv6 :: Misc :: FlowlabelConsistency
Type: Refer to - definitions->types->BooleanInt
Default: 1

2.41.1.5.4.5FlowlabelStateRanges
Property: Sysctl :: Net :: IPv6 :: Misc :: FlowlabelStateRanges
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.5.4.6FwmarkReflect
Property: Sysctl :: Net :: IPv6 :: Misc :: FwmarkReflect
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.5.4.7Icmp
Property: Sysctl :: Net :: IPv6 :: Misc :: Icmp
Type: JSON Object
Default: None

2.41.1.5.4.8Ratelimit
Property: Sysctl :: Net :: IPv6 :: Misc :: Icmp :: Ratelimit
Type: Integer.
Default: 1000

2.41.1.5.4.9IdgenDelay
Property: Sysctl :: Net :: IPv6 :: Misc :: IdgenDelay
Type: Integer.
Default: 1

2.41.1.5.4.10 IdgenRetries
Property: Sysctl :: Net :: IPv6 :: Misc :: IdgenRetries
Type: Integer.
Default: 3

2.41.1.5.4.11 Ip6fragHighThresh
Property: Sysctl :: Net :: IPv6 :: Misc :: Ip6fragHighThresh
Type: Integer.
Default: 4194304

2.41.1.5.4.12 Ip6fragLowThresh
Property: Sysctl :: Net :: IPv6 :: Misc :: Ip6fragLowThresh
Type: Integer.
Default: 3145728

2.41.1.5.4.13 Ip6fragSecretInterval

Property: Sysctl :: Net :: IPv6 :: Misc :: Ip6fragSecretInterval
Type: Integer.
Default: 0

2.41.1.5.4.14 Ip6fragTime
Property: Sysctl :: Net :: IPv6 :: Misc :: Ip6fragTime
Type: Integer with a minimum of 0.
Default: 60

2.41.1.5.4.15 IpNonlocalBind
Property: Sysctl :: Net :: IPv6 :: Misc :: IpNonlocalBind
Type: Refer to - definitions->types->BooleanInt
Default: 0

2.41.1.5.4.16 MldMaxMsf
Property: Sysctl :: Net :: IPv6 :: Misc :: MldMaxMsf
Description: Maximum number of multicast source filters.
Type: Integer with a minimum of 0.
Default: 64

2.41.1.5.4.17 MldQrv
Property: Sysctl :: Net :: IPv6 :: Misc :: MldQrv
Type: Integer.
Default: 2

2.41.1.5.4.18 Xfrm6GcThresh
Property: Sysctl :: Net :: IPv6 :: Misc :: Xfrm6GcThresh
Type: Integer.
Default: 2147483647

2.42 Session

Property: Session
Description: Console session configuration parameters.
Type: JSON Object
Default: None

2.42.1 Lock
Property: Session :: Lock
Description: Remote account lockout settings.
Type: JSON Object
Default: None

2.42.1.1 Attempts
Property: Session :: Lock :: Attempts

Description: The number of failed remote login attempts before the account is locked.
Type: Integer with a minimum of 1 and a maximum of 20.
Default: 3

2.42.1.2 Time
Property: Session :: Lock :: Time
Description: The remote account lockout time (in seconds).
Type: Integer with a minimum of 1 and a maximum of 3600.
Default: 300

2.42.2 Password
Property: Session :: Password
Description: Password complexity requirements.
Type: JSON Object
Default: None

2.42.2.1 DCredit
Property: Session :: Password :: DCredit
Description: The maximum credit for digits in a new password. Negative values for digits that must be met for a new password.
Type: Integer with a minimum of -4 and a maximum of 4.
Default: 0

2.42.2.2 DifOk
Property: Session :: Password :: DifOk
Description: New passwords must differentiate from old passwords by this number of characters (inserts, removals, replacements).
Type: Integer with a minimum of 0 and a maximum of 20.
Default: 0

2.42.2.3 LCredit
Property: Session :: Password :: LCredit
Description: The maximum credit for lower-case characters in a new password. Negative values for minimum lower-case characters that must be met for a new password.
Type: Integer with a minimum of -4 and a maximum of 4.
Default: 0

2.42.2.4 MaxClassRepeat
Property: Session :: Password :: MaxClassRepeat
Description: Reject passwords which contain a consecutive string of characters from a single class (0 to disable).
Type: Integer with a minimum of 0 and a maximum of 20.
Default: 0

2.42.2.5 MaxRepeat
Property: Session :: Password :: MaxRepeat
Description: Reject passwords with consecutive repeating characters (0 to disable).
Type: Integer with a minimum of 0 and a maximum of 20.
Default: 0

2.42.2.6 MaxSequence
Property: Session :: Password :: MaxSequence
Description: Reject passwords with monotonic sequence of characters such as '12345' or 'abcde' (0 to disable).
Type: Integer with a minimum of 0 and a maximum of 20.
Default: 0

2.42.2.7 MinClass
Property: Session :: Password :: MinClass
Description: The minimum number of required character classes in a new password (0 to disable).
Type: Integer with a minimum of 0 and a maximum of 4.
Default: 0

2.42.2.8 MinLength
Property: Session :: Password :: MinLength
Description: The minimum size for a new password.
Type: Integer with a minimum of 6 and a maximum of 100.
Default: 8

2.42.2.9 OCredit
Property: Session :: Password :: OCredit
Description: The maximum credit for "other" characters in a new password. Negative values for minimum "other" characters that must be met for a new password.
Type: Integer with a minimum of -4 and a maximum of 4.
Default: 0

2.42.2.10 UCredit
Property: Session :: Password :: UCredit
Description: The maximum credit for upper case characters in a new password. Negative values for minimum upper-case characters that must be met for a new password.
Type: Integer with a minimum of -4 and a maximum of 4.
Default: 0

2.42.3 Timeout
Property: Session :: Timeout
Description: Console session timeout (in seconds). Remote session timeout is set through SSH server configuration.

Type: Integer with a minimum of 5 and a maximum of 86400.
Default: 900

2.43 SSH

Property: SSH
Description: Configure SSH
Type: JSON Object
Default: None

2.43.1 Client

Property: SSH :: Client
Description: Configuration of a SSH client
Type: Array with a minimum number of 1 item(s).
Item type: JSON Object
Required: ['Host']
Default: None

2.43.1.1 AddressFamily

Property: SSH :: Client :: AddressFamily
Item description: Specifies which address family should be used
Item type: String enum of any, inet, inet6.
Default: any

2.43.1.2 AutoConnect

Property: SSH :: Client :: AutoConnect
Item description: Automatically start a persistent SSH connection to this host. This will default StrictHostKeyChecking=accept-new.
Item type: Boolean true or false.
Default: False

2.43.1.3 BatchMode

Property: SSH :: Client :: BatchMode
Item description: If true, passphrase/password querying will be disabled
Item type: Boolean true or false.
Default: False

2.43.1.4 BindAddress

Property: SSH :: Client :: BindAddress
Item description: Use the specified address on the local machine as the source address of the connection. Only useful on systems with more than one address. Note that this option does not work if UsePrivilegedPort is set to 'yes
Type: Refer to - definitions->types->IPAddress
Default: None

2.43.1.5 BindInterface

Property: SSH :: Client :: BindInterface
Item description: Use the address of the specified interface on the local machine as the source address of the connection
Type: Refer to - definitions->types->InterfaceName
Default: None

2.43.1.6 CanonicalDomains

Property: SSH :: Client :: CanonicalDomains
Item description: When CanonicalizeHostname is enabled, this option specifies the list of domain suffixes in which to search for the specified destination host
Item type: Boolean true or false.
Default: True

2.43.1.7 CanonicalizeFallbackLocal

Property: SSH :: Client :: CanonicalizeFallbackLocal
Item description: Specifies whether to fail with an error when hostname canonicalization fails. The default, yes, will attempt to look up the unqualified hostname using the system resolver's search rules. A value of no will cause ssh to fail instantly if CanonicalizeHostname is enabled and the target hostname cannot be found in any of the domains specified by CanonicalDomains
Item type: Boolean true or false.
Default: True

2.43.1.8 CanonicalizeHostname

Property: SSH :: Client :: CanonicalizeHostname
Item description: Controls whether explicit hostname canonicalization is performed. The default, no, is not to perform any name rewriting and let the system resolver handle all hostname lookups. If set to yes then, for connections that do not use a ProxyCommand or ProxyJump, ssh will attempt to canonicalize the hostname specified on the command line using the CanonicalDomains suffixes and CanonicalizePermittedCNAMEs rules. If CanonicalizeHostname is set to always, then canonicalization is applied to proxied connections too
Item type: Boolean true or false.
Default: True

2.43.1.9 CanonicalizeMaxDots

Property: SSH :: Client :: CanonicalizeMaxDots
Item description: Specifies the maximum number of dot characters in a hostname before canonicalization is disabled. The default, 1, allows a single dot (i.e. hostname.subdomain)
Item type: Integer with a minimum of 0.
Default: 1

2.43.1.10 CanonicalizePermittedCNAMEs

Property: SSH :: Client :: CanonicalizePermittedCNAMEs
Item description: Specifies rules to determine whether CNAMEs should be followed when canonicalizing hostnames. The rules consist of one or more arguments of source_domain_list:target_domain_list, where source_domain_list is a pattern-list of domains that may follow CNAMEs in canonicalization, and target_domain_list is a pattern-list of domains that they may resolve to. For example, '*.a.example.com:*.b.example.com,*.c.example.com' will allow hostnames matching '*.a.example.com' to be canonicalized to names in the '*.b.example.com' or '*.c.example.com' domains. A single argument of 'none' causes no CNAMEs to be considered for canonicalization. This is the default behaviour
Item type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->FQDN_WC
Or
Item type: Enum of none.
Default: none

2.43.1.11 CASignatureAlgorithms

Property: SSH :: Client :: CASignatureAlgorithms
Item description: Specifies which algorithms are allowed for signing of certificates by certificate authorities (CAs)
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256.
Default: ['ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'rsa-sha2-512', 'rsa-sha2-256']

2.43.1.12 CertificateFile

Property: SSH :: Client :: CertificateFile
Item description: Specifies a file from which the user's certificate is read
Type: Refer to - definitions->pki->file
Default: None

2.43.1.13 CheckHostIP

Property: SSH :: Client :: CheckHostIP
Item description: If this flag is set to 'true', ssh will additionally check the host IP address in the known_hosts file. This allows ssh to detect if a host key changed due to DNS spoofing
Item type: Boolean true or false.
Default: True

2.43.1.14 Ciphers

Property: SSH :: Client :: Ciphers
Item description: Specifies the ciphers allowed for protocol version 2 in order of preference
Item type: Array of unique items and a minimum number of 1 item(s).

Item type: Enum of aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com.
Default: ['aes128-cbc', 'aes256-cbc', 'aes128-ctr', 'aes256-ctr', 'aes128-gcm@openssh.com', 'aes256-gcm@openssh.com']

2.43.1.15 ClearAllForwardings

Property: SSH :: Client :: ClearAllForwardings
Item description: Specifies that all local, remote, and dynamic port forwardings specified in the configuration files or on the command line be cleared
Item type: Boolean true or false.
Default: False

2.43.1.16 Compression

Property: SSH :: Client :: Compression
Item description: Specifies whether to use compression
Item type: Boolean true or false.
Default: False

2.43.1.17 ConnectionAttempts

Property: SSH :: Client :: ConnectionAttempts
Item description: Specifies the number of tries (one per second) to make before exiting
Item type: Integer with a minimum of 0.
Default: 1

2.43.1.18 ConnectTimeout

Property: SSH :: Client :: ConnectTimeout
Item description: Specifies the timeout (in seconds) used when connecting to the SSH server, instead of using the default system TCP timeout
Item type: Integer with a minimum of 0.
Default: None

2.43.1.19 DynamicForward

Property: SSH :: Client :: DynamicForward
Item description: Specifies that a TCP port on the local machine be forwarded over the secure channel (the SSH client acts as a SOCKS proxy), and the application protocol is then used to determine where to connect to from the remote machine.
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Default: None

2.43.1.19.1 BindAddress

Property: SSH :: Client :: DynamicForward :: BindAddress
Item description: The address to bind to on the local machine.
Type: Refer to - definitions->types->IPAddress

Default: None

2.43.1.19.2 Port

Property: SSH :: Client :: DynamicForward :: Port
Item description: The port to forward over the secure channel.
Type: Refer to - definitions->types->Port
Default: None

2.43.1.20 EnableSSHKeysign

Property: SSH :: Client :: EnableSSHKeysign
Item description: Enables the use of the helper program ssh-keysign during HostbasedAuthentication
Item type: Boolean true or false.
Default: False

2.43.1.21 EscapeChar

Property: SSH :: Client :: EscapeChar
Item description: Sets the escape character. The escape character can also be set on the command line. The argument should be a single character, '^' followed by a letter, or 'none' to disable the escape character entirely (making the connection transparent for binary data).
Item type: String pattern of ^([!-~]|\^[a-zA-Z]|none)$.
Default: ~

2.43.1.22 ExitOnForwardFailure

Property: SSH :: Client :: ExitOnForwardFailure
Item description: Specifies whether ssh should terminate the connection if it cannot set up all requested dynamic, tunnel, local, and remote port forwardings
Item type: Boolean true or false.
Default: False

2.43.1.23 FingerprintHash

Property: SSH :: Client :: FingerprintHash
Item description: Specifies the hash algorithm used when displaying key fingerprints
Item type: Enum of md5, sha256.
Default: sha256

2.43.1.24 ForwardAgent

Property: SSH :: Client :: ForwardAgent
Item description: Specifies whether the connection to the authentication agent (if any) will be forwarded to the remote machine
Item type: Boolean true or false.
Default: False

2.43.1.25 GatewayPorts

Property: SSH :: Client :: GatewayPorts
Item description: Specifies whether remote hosts are allowed to connect to local forwarded ports
Item type: Boolean true or false.
Default: False

2.43.1.26 HashKnownHosts

Property: SSH :: Client :: HashKnownHosts
Item description: Indicates that ssh should hash host names and addresses. These hashed names may be used normally by ssh and sshd, but they do not reveal identifying information should the file's contents be disclosed. Note that existing names and addresses in known hosts files will not be converted automatically, but may be manually hashed using ssh-keygen
Item type: Boolean true or false.
Default: False

2.43.1.27 HostbasedAcceptedAlgorithms

Property: SSH :: Client :: HostbasedAcceptedAlgorithms
Item description: Specifies the signature algorithms that will be used for hostbased authentication
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.
Default: ['ssh-rsa', 'rsa-sha2-256', 'rsa-sha2-512', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521']

2.43.1.28 HostbasedAuthentication

Property: SSH :: Client :: HostbasedAuthentication
Item description: Specifies whether to try rhosts based authentication with public key authentication. This option applies to protocol version 2 only and is similar to RhostsRSAAuthentication
Item type: Boolean true or false.
Default: False

2.43.1.29 HostKeyAlgorithms

Property: SSH :: Client :: HostKeyAlgorithms
Item description: Specifies the host key signature algorithms that the server offers
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.
Default: ['ssh-rsa', 'rsa-sha2-256', 'rsa-sha2-512', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521']

2.43.1.30 HostKeyAlias

Property: SSH :: Client :: HostKeyAlias

Item description: Specifies an alias that should be used instead of the real host name when looking up or saving the host key in the host key database files. This option is useful for tunneling SSH connections or for multiple servers running on a single host
Item type: String.
Default: None

2.43.1.31 Host

Property: SSH :: Client :: Host
Item description: Host to apply settings for. IP, FQDN, or nickname (if used together with Hostname).
Or
Type: Refer to - definitions->types->IPAddress
Type: Refer to - definitions->types->FQDN
Or
Item type: String pattern of ^([a-zA-Z0-9_-]{1-20}|*)$.
Default: None

2.43.1.32 Hostname

Property: SSH :: Client :: Hostname
Item description: Specifies the real host name to log into. This can be used to specify nicknames or abbreviations for hosts. Numeric IP addresses are also permitted
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.1.33 IdentityFile

Property: SSH :: Client :: IdentityFile
Item description: Specifies file(s) from which the RSA or ECDSA authentication identity to be used is read.
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item description: Name of identity read from current user ".ssh/" directory.
Type: Refer to - definitions->types->AlphaNumeric
Or
Item description: Relative path to a file from which the SSH private key is read, only used for automatic connections.
Item type: String pattern of ^file://((rsa|ecdsa|private)/)?[a-zA-Z0-9_ \.\-]+(\.key)?$.
Default: None

2.43.1.34 IPQoS

Property: SSH :: Client :: IPQoS
Item description: Specifies the IPv4 type-of-service or DSCP class for connections. This option may take one or two arguments. If one argument is specified, it is used as the packet class

unconditionally. If two values are specified, the first is automatically selected for interactive sessions and the second for non-interactive sessions
Item type: Array of unique items and a minimum number of 1 item(s) and a maximum number of 2 item(s).
Item type: String pattern of ^([0-9]|[1-5][0-9]|6[0-3])$.
Or
Item type: Enum of af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef, le, lowdelay, throughput, reliability, none.
Default: ['none']

2.43.1.35 KbdInteractiveAuthentication

Property: SSH :: Client :: KbdInteractiveAuthentication
Item description: Specifies whether to use keyboard-interactive authentication
Item type: Boolean true or false.
Default: True

2.43.1.36 KbdInteractiveDevices

Property: SSH :: Client :: KbdInteractiveDevices
Item description: Specifies the list of methods to use in keyboard-interactive authentication
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of bsdauth, pam, skey.
Default: None

2.43.1.37 KexAlgorithms

Property: SSH :: Client :: KexAlgorithms
Item description: Specifies the available KEX (Key Exchange) algorithms
Item type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.
Default: ['diffie-hellman-group14-sha1', 'diffie-hellman-group14-sha256', 'diffie-hellman-group16-sha512', 'diffie-hellman-group18-sha512', 'ecdh-sha2-nistp256', 'ecdh-sha2-nistp384', 'ecdh-sha2-nistp521']

2.43.1.38 LocalForward

Property: SSH :: Client :: LocalForward
Item description: Specifies that a TCP port on the local machine be forwarded over the secure channel to the specified host and port from the remote machine
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Default: None

2.43.1.38.1 BindAddress

Property: SSH :: Client :: LocalForward :: BindAddress

Item description: The address to bind to on the local machine. If not set, indicates that the port should be available from all interfaces.
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.1.38.2 Port
Property: SSH :: Client :: LocalForward :: Port
Item description: The local TCP port to forward over the secure channel
Type: Refer to - definitions->types->Port
Default: None

2.43.1.38.3 Host
Property: SSH :: Client :: LocalForward :: Host
Item description: The IP address or FQDN of the destination host
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.1.38.4 HostPort
Property: SSH :: Client :: LocalForward :: HostPort
Item description: The remote port to forward traffic to
Type: Refer to - definitions->types->Port
Default: None

2.43.1.39 LogLevel
Property: SSH :: Client :: LogLevel
Item description: Gives the verbosity level that is used when logging messages from ssh
Item type: Enum of INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, DEBUG3.
Default: VERBOSE

2.43.1.40 MACs
Property: SSH :: Client :: MACs
Item description: Specifies the MAC (message authentication code) algorithms in order of preference. The MAC algorithm is used in protocol version 2 for data integrity protection
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512.
Default: ['hmac-sha2-256', 'hmac-sha2-512', 'hmac-sha1-96', 'hmac-sha1']

2.43.1.41 NoHostAuthenticationForLocalhost
Property: SSH :: Client :: NoHostAuthenticationForLocalhost

Item description: This option can be used if the home directory is shared across machines. In this case localhost will refer to a different machine on each of the machines and the user will get many warnings about changed host keys. However, this option disables host authentication for localhost
Item type: Boolean true or false.
Default: None

2.43.1.42 NumberOfPasswordPrompts

Property: SSH :: Client :: NumberOfPasswordPrompts
Item description: Specifies the number of password prompts before giving up
Item type: Integer with a minimum of 0.
Default: 3

2.43.1.43 PermitRemoteOpen

Property: SSH :: Client :: PermitRemoteOpen
Item description: Specifies the destinations to which remote TCP port forwarding is permitted when RemoteForward is used as a SOCKS proxy
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Default: None

2.43.1.43.1 Host

Property: SSH :: Client :: PermitRemoteOpen :: Host
Item description: The IP address or FQDN of the destination host
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.1.43.2 Port

Property: SSH :: Client :: PermitRemoteOpen :: Port
Item description: The port to allow forwarding to on the destination host
Type: Refer to - definitions->types->Port
Default: None

2.43.1.44 Port

Property: SSH :: Client :: Port
Item description: Specifies the port number to connect on the remote host
Type: Refer to - definitions->types->Port
Default: 22

2.43.1.45 PreferredAuthentications

Property: SSH :: Client :: PreferredAuthentications

Item description: Specifies the order in which the client should try protocol 2 authentication methods. This allows a client to prefer one method (e.g. keyboard-interactive) over another method (e.g. password)
Item type: Array of unique items and a minimum number of 1 item(s).
Default: None

2.43.1.46 PubkeyAcceptedAlgorithms

Property: SSH :: Client :: PubkeyAcceptedAlgorithms
Item description: Specifies the signature algorithms that will be used for public key authentication
Item type: Array of unique items and a minimum number of 1 item(s).
Default: None

2.43.1.47 PubkeyAuthentication

Property: SSH :: Client :: PubkeyAuthentication
Item description: Specifies whether to try public key authentication
Item type: Enum of host-bound, no, unbound, yes.
Default: yes

2.43.1.48 RekeyLimit

Property: SSH :: Client :: RekeyLimit
Item description: Specifies the maximum time and amount of data that may be transmitted before the session key is renegotiated. This option applies to protocol version 2 only.
Item type: JSON Object
Default: None

2.43.1.48.1 MaxData

Property: SSH :: Client :: RekeyLimit :: MaxData
Item description: Maximum amount of data transmitted before the session key is renegotiated. Specified in kilobytes, megabytes, or gigabytes with a corresponding suffix of 'K', 'M', or 'G'. The default is between '1G' and '4G', depending on the cipher and security mode.
Item type: String.
Or
Item type: String pattern of ^([1-9]|[1-9][0-9]{1,5}|1000000)[kK]$.
Item type: String pattern of ^([1-9]|[1-9][0-9]{1,2}|1000)[mM]$.
Or
Item type: String pattern of ^1[gG]$.
Default: None

2.43.1.48.2 MaxTime

Property: SSH :: Client :: RekeyLimit :: MaxTime
Item description: Maximum amount of time that may pass before the session key is renegotiated. Specified in seconds, minutes, or hours with a corresponding suffix of 's', 'm', or 'h'. If no suffix is provided, the default format is seconds.

Item type: String.
Or
Item type: String pattern of ^([1-9]|[1-9][0-9]{1,2}|[12][0-9]{3}|3[0-5][0-9]{2}|3600)[sS]?$.
Item type: String pattern of ^([1-9]|[1-5][0-9]|60)[mM]$.
Or
Item type: String pattern of ^1[hH]$.
Default: None

2.43.1.49 RemoteForward

Property: SSH :: Client :: RemoteForward
Item description: Specifies that a TCP port on the remote machine be forwarded over the secure channel to the specified host and port from the local machine. If no destination is specified, the remote forwarding will be established as a SOCKS proxy. When acting as a SOCKS proxy, allowable destination addresses can be restricted by PermitRemoteOpen.
Item type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Default: None

2.43.1.49.1 BindAddress

Property: SSH :: Client :: RemoteForward :: BindAddress
Item description: The listening address to bind to on the remote machine. If not set, the default is to only bind to loopback addresses.
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.1.49.2 Port

Property: SSH :: Client :: RemoteForward :: Port
Item description: The remote TCP port to forward over the secure channel.
Type: Refer to - definitions->types->Port
Default: None

2.43.1.49.3 Host

Property: SSH :: Client :: RemoteForward :: Host
Item description: The host to forward traffic to.
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.1.49.4 HostPort

Property: SSH :: Client :: RemoteForward :: HostPort
Item description: The port to forward traffic to.

Type: Refer to - definitions->types->Port
Default: None

2.43.1.50 RequestTTY

Property: SSH :: Client :: RequestTTY
Item description: Specifies whether to request a pseudo-tty for the session
Item type: Enum of auto, force, no, yes.
Default: None

2.43.1.51 RequiredRSASize

Property: SSH :: Client :: RequiredRSASize
Item description: Specifies the minimum RSA key size (in bits) that ssh will accept. User authentication keys smaller than this limit will be ignored. Servers that present host keys smaller than this limit will cause the connection to be terminated
Item type: Integer with a minimum of 512.
Default: 1024

2.43.1.52 ServerAliveCountMax

Property: SSH :: Client :: ServerAliveCountMax
Item description: Sets the number of server alive messages which may be sent without ssh receiving any messages back from the server. This option applies to protocol version 2 only
Item type: Integer with a minimum of 0.
Default: 3

2.43.1.53 ServerAliveInterval

Property: SSH :: Client :: ServerAliveInterval
Item description: Sets a timeout interval in seconds after which if no data has been received from the server, ssh will send a message through the encrypted channel to request a response from the server. This option applies to protocol version 2 only
Item type: Integer with a minimum of 0.
Default: 0

2.43.1.54 StrictHostKeyChecking

Property: SSH :: Client :: StrictHostKeyChecking
Item description: If this flag is set to 'yes', ssh will never automatically add host keys to the known_hosts file, and refuses to connect to hosts whose host key has changed. This provides maximum protection against trojan horse attacks, though it can be annoying when the known_hosts file is poorly maintained or when connections to new hosts are frequently made. This option forces the user to manually add all new hosts. If this flag is set to 'no', ssh will automatically add new host keys to the user known hosts files. If this flag is set to 'ask', new host keys will be added to the user known host files only after the user has confirmed that is what they really want to do, and ssh will refuse to connect to hosts whose host key has changed. The host keys of known hosts will be verified automatically in all cases
Item type: Enum of ask, no, yes, accept-new.

Default: ask

2.43.1.55 TCPKeepAlive

Property: SSH :: Client :: TCPKeepAlive
Item description: Specifies whether the system should send TCP keepalive messages to the other side. If they are sent, death of the connection or crash of one of the machines will be properly noticed
Item type: Boolean true or false.
Default: True

Tunnel

2.43.1.56 Property: SSH :: Client :: Tunnel

Item description: Request tun device forwarding between the client and the server
Item type: Enum of ethernet, no, point-to-point, yes.
Default: no

2.43.1.57 TunnelDevice

Property: SSH :: Client :: TunnelDevice
Item description: Specifies the tun devices to open on the client and the server
Item type: JSON Object
Default: None

2.43.1.57.1 Local

Property: SSH :: Client :: TunnelDevice :: Local
Item description: Local
Type: Refer to - definitions->types->InterfaceName
Default: any

2.43.1.57.2 Remote

Property: SSH :: Client :: TunnelDevice :: Remote
Item description: Remote
Type: Refer to - definitions->types->InterfaceName
Default: any

2.43.1.58 User

Property: SSH :: Client :: User
Item description: Specifies the user to log in as. This can be useful when a different user name is used on different machines
Item type: String.
Default: None

2.43.1.59 VerifyHostKeyDNS

Property: SSH :: Client :: VerifyHostKeyDNS

Item description: Specifies whether to verify the remote key using DNS and SSHFP resource records. If this option is set to 'true', the client will implicitly trust keys that match a secure fingerprint from DNS. Insecure fingerprints will be handled as if this option was set to 'ask'. If this option is set to 'ask', information on fingerprint match will be displayed, but the user will still need to confirm new host keys according to the StrictHostKeyChecking option. Note that this option applies to protocol version 2 only
Item type: Enum of ask, no, yes.
Default: no

2.43.1.60 VisualHostKey

Property: SSH :: Client :: VisualHostKey
Item description: If this flag is set to 'true', an ASCII art representation of the remote host key fingerprint is printed in addition to the hex fingerprint string at login and for unknown host keys. If this flag is set to 'false', no fingerprint strings are printed at login and only the hex fingerprint string will be printed for unknown host keys
Item type: Boolean true or false.
Default: False

2.43.2 Server

Property: SSH :: Server
Description: Configuration of a SSH server
Type: JSON Object
Default: None

2.43.2.1 AddressFamily

Property: SSH :: Server :: AddressFamily
Description: Specifies which address family should be used
Type: Enum of any, inet, inet6.
Default: any

2.43.2.2 AllowStreamLocalForwarding

Property: SSH :: Server :: AllowStreamLocalForwarding
Description: Specifies whether StreamLocal (Unix-domain socket) forwarding is permitted
Type: String enum of all, local, no, remote, yes.
Default: yes

2.43.2.3 AllowTcpForwarding

Property: SSH :: Server :: AllowTcpForwarding
Description: Specifies whether TCP forwarding is permitted
Type: String enum of all, local, no, remote, yes.
Default: no

2.43.2.4 AuthenticationMethods

Property: SSH :: Server :: AuthenticationMethods

Description: Specifies the authentication methods that must be successfully completed for a user to be granted access
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of any, hostbased, keyboard-interactive, none, password, publickey.
Default: None

2.43.2.5 CASignatureAlgorithms

Property: SSH :: Server :: CASignatureAlgorithms
Description: Specifies which algorithms are allowed for signing of certificates by certificate authorities
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: Enum of ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256.
Default: ['ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'rsa-sha2-512', 'rsa-sha2-256']

2.43.2.6 ChannelTimeout

Property: SSH :: Server :: ChannelTimeout
Description: Specifies whether and how quickly sshd should close inactive channels. The timeout value “interval” is specified in seconds or may use any of the time units. Specifying a zero value disables the inactivity timeout
Type: String pattern of ^[1-9][0-9]{0,8}[sSmMhHdDwW]?$.
Default: None

2.43.2.7 Ciphers

Property: SSH :: Server :: Ciphers
Description: Specifies the ciphers allowed
Type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com.
Default: ['aes128-cbc', 'aes256-cbc', 'aes128-ctr', 'aes256-ctr', 'aes128-gcm@openssh.com', 'aes256-gcm@openssh.com']

2.43.2.8 ClientAliveCountMax

Property: SSH :: Server :: ClientAliveCountMax
Description: Sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option enabled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive
Type: Integer with a minimum of 0.
Default: 0

2.43.2.9 ClientAliveInterval

Property: SSH :: Server :: ClientAliveInterval
Description: Sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client
Type: Integer with a minimum of 0.
Default: 300

2.43.2.10 Compression

Property: SSH :: Server :: Compression
Description: Specifies whether compression is enabled after the user has authenticated successfully
Type: Enum of delayed, no, yes.
Default: yes

2.43.2.11 DisableForwarding

Property: SSH :: Server :: DisableForwarding
Description: Disables all forwarding features, including X11, ssh-agent, TCP and StreamLocal. This option overrides all other forwarding related options and may simplify restricted configurations
Type: Boolean true or false.
Default: False

2.43.2.12 Enable

Property: SSH :: Server :: Enable
Description: Enable a SSH server
Type: Boolean true or false.
Default: True

2.43.2.13 FingerprintHash

Property: SSH :: Server :: FingerprintHash
Description: Specifies the hash algorithm used when logging key fingerprints
Type: Enum of md5, sha256.
Default: sha256

2.43.2.14 GatewayPorts

Property: SSH :: Server :: GatewayPorts
Description: Specifies whether remote hosts are allowed to connect to ports forwarded for the client. By default, sshd binds remote port forwardings to the loopback address
Type: String enum of clientspecified, no, yes.
Default: no

2.43.2.15 HostbasedAcceptedAlgorithms

Property: SSH :: Server :: HostbasedAcceptedAlgorithms
Description: Specifies the signature algorithms that will be accepted for hostbased authentication
Type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.
Default: ['diffie-hellman-group14-sha1', 'diffie-hellman-group14-sha256', 'diffie-hellman-group16-sha512', 'diffie-hellman-group18-sha512', 'ecdh-sha2-nistp256', 'ecdh-sha2-nistp384', 'ecdh-sha2-nistp521']

2.43.2.16 HostbasedAuthentication

Property: SSH :: Server :: HostbasedAuthentication
Description: Specifies whether rhosts or hosts.equiv authentication together with successful public key client host authentication is allowed (host-based authentication)
Type: Boolean true or false.
Default: False

2.43.2.17 HostbasedUsesNameFromPacketOnly

Property: SSH :: Server :: HostbasedUsesNameFromPacketOnly
Description: Specifies whether or not the server will attempt to perform a reverse name lookup when matching the name
Type: Boolean true or false.
Default: False

2.43.2.18 HostCertificate

Property: SSH :: Server :: HostCertificate
Description: Specifies a public host certificate. The certificate's public key must match a private host key already specified by HostKey
Type: Refer to - definitions->pki->file
Default: None

2.43.2.19 HostKey

Property: SSH :: Server :: HostKey
Description: Specifies a file containing a private host key used by SSH
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->pki->file
Default: None

2.43.2.20 HostKeyAlgorithms

Property: SSH :: Server :: HostKeyAlgorithms
Description: Specifies the host key signature algorithms that the server offers
Type: Array of unique items and a minimum number of 1 item(s).

Item type: Enum of diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.
Default: ['diffie-hellman-group14-sha1', 'diffie-hellman-group14-sha256', 'diffie-hellman-group16-sha512', 'diffie-hellman-group18-sha512', 'ecdh-sha2-nistp256', 'ecdh-sha2-nistp384', 'ecdh-sha2-nistp521']

2.43.2.21 IgnoreUserKnownHosts

Property: SSH :: Server :: IgnoreUserKnownHosts
Description: Specifies whether sshd should ignore the user's known_hosts during HostbasedAuthentication and use only the system-wide known hosts file
Type: Boolean true or false.
Default: False

2.43.2.22 IPQoS

Property: SSH :: Server :: IPQoS
Description: Specifies the IPv4 type-of-service or DSCP class for connections. This option may take one or two arguments. If one argument is specified, it is used as the packet class unconditionally. If two values are specified, the first is automatically selected for interactive sessions and the second for non-interactive sessions
Type: Array of unique items and a minimum number of 1 item(s) and a maximum number of 2 item(s).
Item type: String pattern of ^([0-9]|[1-5][0-9]|6[0-3])$.
Or
Item type: Enum of af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef, le, lowdelay, throughput, reliability, none.
Default: ['none']

2.43.2.23 KbdInteractiveAuthentication

Property: SSH :: Server :: KbdInteractiveAuthentication
Description: Specifies whether to allow keyboard-interactive authentication
Type: Boolean true or false.
Default: True

2.43.2.24 KexAlgorithms

Property: SSH :: Server :: KexAlgorithms
Description: Specifies the available KEX (Key Exchange) algorithms
Type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.
Default: ['diffie-hellman-group14-sha1', 'diffie-hellman-group14-sha256', 'diffie-hellman-group16-sha512', 'diffie-hellman-group18-sha512', 'ecdh-sha2-nistp256', 'ecdh-sha2-nistp384', 'ecdh-sha2-nistp521']

2.43.2.25 ListenAddress

Property: SSH :: Server :: ListenAddress
Description: Specifies one or more local addresses sshd should listen on
Type: Array with a minimum number of 1 item(s) that must be unique.
Item description: A local address sshd should listen on
Item type: JSON Object
Default: None

2.43.2.25.1 Address

Property: SSH :: Server :: ListenAddress :: Address
Item description: IPv4/v6 address or FQDN
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.2.25.2 Port

Property: SSH :: Server :: ListenAddress :: Port
Item description: Port to listen on [1-49151]
Type: Refer to - definitions->types->Port
Default: None

2.43.2.26 LoginGraceTime

Property: SSH :: Server :: LoginGraceTime
Description: The server disconnects after this time if the user has not successfully logged in
Type: Integer with a minimum of 0.
Default: 120

2.43.2.27 LogLevel

Property: SSH :: Server :: LogLevel
Description: Gives the verbosity level that is used when logging messages from sshd
Type: Enum of INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, DEBUG3.
Default: VERBOSE

2.43.2.28 MACs

Property: SSH :: Server :: MACs
Description: Specifies the available KEX (Key Exchange) algorithms
Type: Array of unique items and a minimum number of 1 item(s) -MaxAuthTries- -MaxSessions- .
Item type: Enum of hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512.
Default: ['hmac-sha2-256', 'hmac-sha2-512', 'hmac-sha1-96', 'hmac-sha1']

2.43.2.28.1 MaxAuthTries
Property: SSH :: Server :: MACs :: MaxAuthTries
Default: 6

2.43.2.28.2 MaxSessions
Property: SSH :: Server :: MACs :: MaxSessions
Default: 10

2.43.2.29 MaxAuthTries
Property: SSH :: Server :: MaxAuthTries
Description: Specifies the maximum number of authentication attempts permitted per connection
Type: Integer.
Default: None

2.43.2.30 MaxSessions
Property: SSH :: Server :: MaxSessions
Description: Specifies the maximum number of open shell, login or subsystem (e.g. sftp) sessions permitted per network connection
Type: Integer.
Default: None

2.43.2.31 MaxStartups
Property: SSH :: Server :: MaxStartups
Description: Specifies the maximum number of concurrent unauthenticated connections to the SSH daemon
Type: JSON Object
Default: None

2.43.2.31.1 Start
Property: SSH :: Server :: MaxStartups :: Start
Description: Start
Type: Integer with a minimum of 0.
Default: None

2.43.2.31.2 Rate
Property: SSH :: Server :: MaxStartups :: Rate
Description: Rate
Type: Integer with a minimum of 0.
Default: None

2.43.2.31.3 Full
Property: SSH :: Server :: MaxStartups :: Full
Description: Full

Type: Integer with a minimum of 0.
Default: None

2.43.2.32 PasswordAuthentication

Property: SSH :: Server :: PasswordAuthentication
Description: Specifies whether password authentication is allowed
Type: Boolean true or false.
Default: False

2.43.2.33 PermitListen

Property: SSH :: Server :: PermitListen
Description: Specifies one or more addresses/ports on which a remote TCP port forwarding may listen
Type: Array with a minimum number of 1 item(s) that must be unique.
Item description: Specifies the address/port on which a remote TCP port forwarding may listen
Item type: JSON Object
Default: None

2.43.2.33.1 Address

Property: SSH :: Server :: PermitListen :: Address
Item description: Address
Type: Refer to - definitions->types->IPAddress
Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.2.33.2 Port

Property: SSH :: Server :: PermitListen :: Port
Item description: Port
Type: Refer to - definitions->types->Port
Default: None

2.43.2.34 PermitOpen

Property: SSH :: Server :: PermitOpen
Description: Specifies one or more destinations to which TCP port forwarding is permitted
Type: Array with a minimum number of 1 item(s) that must be unique.
Item description: Specifies the destination to which TCP port forwarding is permitted
Item type: JSON Object
Default: None

2.43.2.34.1 Address

Property: SSH :: Server :: PermitOpen :: Address
Item description: Address
Type: Refer to - definitions->types->IPAddress

Or
Type: Refer to - definitions->types->FQDN
Default: None

2.43.2.34.2 Port
Property: SSH :: Server :: PermitOpen :: Port
Item description: Port
Type: Refer to - definitions->types->Port
Default: None

2.43.2.35 PermitTTY
Property: SSH :: Server :: PermitTTY
Description: Specifies whether pty allocation is permitted.
Type: Boolean true or false.
Default: True

2.43.2.36 PermitTunnel
Property: SSH :: Server :: PermitTunnel
Description: Specifies whether tun device forwarding is allowed
Type: Enum of ethernet, no, point-to-point, yes.
Default: no

2.43.2.37 Ports
Property: SSH :: Server :: Ports
Description: Specifies the port numbers that sshd listens on
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->types->Port
Default: None

2.43.2.38 PrintLastLog
Property: SSH :: Server :: PrintLastLog
Description: Specifies whether sshd should print the date and time of the last user login when a user logs in interactively
Type: Boolean true or false.
Default: True

2.43.2.39 PubkeyAcceptedAlgorithms
Property: SSH :: Server :: PubkeyAcceptedAlgorithms
Description: Specifies the signature algorithms that will be accepted for public key authentication
Type: Array of unique items and a minimum number of 1 item(s).
Item type: Enum of ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256.

Default: ['ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'rsa-sha2-512', 'rsa-sha2-256']

2.43.2.40 PubkeyAuthentication

Property: SSH :: Server :: PubkeyAuthentication
Description: Specifies whether public key authentication is allowed
Type: Boolean true or false.
Default: False

2.43.2.41 RekeyLimit

Property: SSH :: Server :: RekeyLimit
Description: Specifies the maximum time and amount of data that may be transmitted before the session key is renegotiated. This option applies to protocol version 2 only.
Type: JSON Object
Default: None

2.43.2.41.1 MaxData

Property: SSH :: Server :: RekeyLimit :: MaxData
Description: Maximum amount of data transmitted before the session key is renegotiated. Specified in kilobytes, megabytes, or gigabytes with a corresponding suffix of 'K', 'M', or 'G'. The default is between '1G' and '4G', depending on the cipher and security mode.
Type: String.
Or
Type: String pattern of ^([1-9]|[1-9][0-9]{1,5}|1000000)[kK]$.
Type: String pattern of ^([1-9]|[1-9][0-9]{1,2}|1000)[mM]$.
Or
Type: String pattern of ^1[gG]$.
Default: None

2.43.2.41.2 MaxTime

Property: SSH :: Server :: RekeyLimit :: MaxTime
Description: Maximum amount of time that may pass before the session key is renegotiated. Specified in seconds, minutes, or hours with a corresponding suffix of 's', 'm', or 'h'. If no suffix is provided, the default format is seconds.
Type: String.
Or
Type: String pattern of ^([1-9]|[1-9][0-9]{1,2}|[12][0-9]{3}|3[0-5][0-9]{2}|3600)[sS]?$.
Type: String pattern of ^([1-9]|[1-5][0-9]|60)[mM]$.
Or
Type: String pattern of ^1[hH]$.
Default: None

2.43.2.42 RequiredRSASize

Property: SSH :: Server :: RequiredRSASize

Description: Specifies the minimum RSA key size (in bits) that sshd will accept. User and host-based authentication keys smaller than this limit will be refused
Type: Integer with a minimum of 512.
Default: 1024

2.43.2.43 SyslogFacility

Property: SSH :: Server :: SyslogFacility
Description: Gives the facility code that is used when logging messages from sshd
Type: Enum of AUTH, DAEMON, LOCAL0, LOCAL1, LOCAL2, LOCAL4, LOCAL5, LOCAL6, LOCAL7, USER.
Default: AUTH

2.43.2.44 TCPKeepAlive

Property: SSH :: Server :: TCPKeepAlive
Description: Specifies whether the system should send TCP keepalive messages to the other side
Type: Boolean true or false.
Default: True

2.43.2.45 UnusedConnectionTimeout

Property: SSH :: Server :: UnusedConnectionTimeout
Description: Specifies whether and how quickly sshd should close client connections with no open channels
Or
Item type: Enum of none.
Default: none
Or
Type: String pattern of ^[1-9][0-9]{0,8}[sSmMhHdDwW]?$.
Default: None

2.43.2.46 UseDNS

Property: SSH :: Server :: UseDNS
Description: Specifies whether sshd should look up the remote host name and check that the resolved host name for the remote IP address maps back to the very same IP address
Type: Boolean true or false.
Default: True

2.44 SNMP

Property: SNMP
Description: SNMP server
Type: JSON Object
Default: None

2.44.1 Enable
Property: SNMP :: Enable
Description: Enable SNMP server.
Type: Boolean true or false.
Default: False

2.44.2 SysInfo
Property: SNMP :: SysInfo
Description: Allow SNMP public information.
Type: Boolean true or false.
Default: True

2.44.3 sysName
Property: SNMP :: sysName
Description: The system name.
Type: String.
Default: None

2.44.4 sysDescr
Property: SNMP :: sysDescr
Description: Optional discription for system.
Type: String.
Default: None

2.44.5 sysLocation
Property: SNMP :: sysLocation
Description: The [physical] location of the system.
Type: String.
Default: None

2.44.6 sysContact
Property: SNMP :: sysContact
Description: Contact info for system admin.
Type: String.
Default: None

2.44.7 sysServices
Property: SNMP :: sysServices
Description: The proper value for the sysServices object.
Type: Refer to - definitions->types->UINT32
Default: 72

2.44.8 Views
Property: SNMP :: Views
Description: Specify views to be accessible via the running SNMP server.
Type: Array of unique items and a minimum number of 0 item(s).
Item description: arguments viewname included [oid]
Item type: JSON Object
Required: ['Name', 'InclExcl', 'Subtree']
Default: None

2.44.8.1 Name
Property: SNMP :: Views :: Name
Item description: What is viewable, i.e. 'all'
Item type: String.
Default: None

2.44.8.2 InclExcl
Property: SNMP :: Views :: InclExcl
Item description: Include/Exclude view
Item type: String enum of included, excluded.
Default: None

2.44.8.3 Subtree
Property: SNMP :: Views :: Subtree
Item description: An object identifier
Item type: String.
Default: None

2.44.9 agentaddress
Property: SNMP :: agentaddress
Description: IP address and port number the agent will listen on. Listen to all interfaces on port 161 by default.
Type: JSON Object
Default: None

2.44.9.1 IPAddress
Property: SNMP :: agentaddress :: IPAddress
Description: IP Address, leave blank to use any interface.
Type: Refer to - definitions->types->IPAddress
Default: None

2.44.9.2 Port
Property: SNMP :: agentaddress :: Port
Description: Port number
Type: Refer to - definitions->types->Port

Default: 161

2.44.10rocommunity
Property: SNMP :: rocommunity
Description: SNMPv1 read-only access community name
Type: String.
Default: public default

2.44.11rocommunity6
Property: SNMP :: rocommunity6
Description: SNMPv2c read-only access community name
Type: String.
Default: public default

2.44.12rouser
Property: SNMP :: rouser
Description: SNMPv3 read-only access username
Type: String.
Default: authPrivUser authpriv -V systemonly

2.45 Accounts

Property: Accounts
Description: Array of accounts that will be created or updated. If an account specified is does not exist, it will created. If an account specified exists but the group and/or password differ, its group and/or password will be updated.
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->accounts->AccountObject
Default: None

2.46 FIND

Property: FIND
Description: Information to return upon receipt of Find Information of Network Devices (FIND) request
Type: JSON Object
Required: ['ID', 'Type', 'Position']
Default: None

2.46.1 ID
Property: FIND :: ID
Description: Target hardware ID
Type: String pattern of ^[a-zA-Z0-9]{1,12}$.
Default: None

2.46.2 Type
Property: FIND :: Type
Description: Target hardware type
Type: String pattern of ^[a-zA-Z0-9]{1,8}$.
Default: None

2.46.3 Position
Property: FIND :: Position
Description: Target hardware position (e.g.: "LEFT")
Type: String pattern of ^[a-zA-Z0-9]{1,8}$.

3 Configuration Parameter Definitions

3.1 General Type Definitions

3.1.1 HardwareAddress
Property: definitions :: types :: HardwareAddress
Type: String pattern of ^([0-9A-Fa-f]{2}:){5}([0-9A-Fa-f]{2})$.
Default: None

3.1.2 HardwareAddressArr
Property: definitions :: types :: HardwareAddressArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->HardwareAddress
Default: None

3.1.3 DUID
Property: definitions :: types :: DUID
Type: String pattern of ^([0-9A-Fa-f]{2}:){2,129}([0-9A-Fa-f]{2})$.
Default: None

3.1.4 DottedQuad
Property: definitions :: types :: DottedQuad
Type: String pattern of ^((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)$.
Default: None

3.1.5 DottedQuadMaskReq
Property: definitions :: types :: DottedQuadMaskReq
Type: String pattern of ^((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)/(3[0-2]|[1-2]?\d)$.
Default: None

3.1.6 DottedQuadRange
Property: definitions :: types :: DottedQuadRange
Type: String pattern of ^((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)-((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)$.
Default: None

3.1.7 DottedQuadRangeMaskReq
Property: definitions :: types :: DottedQuadRangeMaskReq
Type: String pattern of ^(\((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)-(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\)\.|(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(\((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)-(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\)|(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d))/(3[0-2]|[1-2]?\d)$.
Default: None

3.1.8 DottedQuadMaskOpt
Property: definitions :: types :: DottedQuadMaskOpt
Type: Refer to - definitions->types->DottedQuad
Or
Type: Refer to - definitions->types->DottedQuadMaskReq
Default: None

3.1.9 IPv4Multicast
Property: definitions :: types :: IPv4Multicast
Type: String pattern of ^(23\d|22[4-9])\.((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){2}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)$.
Default: None

3.1.10 IPv4MulticastMaskReq
Property: definitions :: types :: IPv4MulticastMaskReq
Type: String pattern of ^(23\d|22[4-9])\.((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){2}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)/(3[0-2]|[1-2]?\d)$.
Default: None

3.1.11 IPv4MulticastMaskOpt
Property: definitions :: types :: IPv4MulticastMaskOpt
Type: Refer to - definitions->types->IPv4Multicast
Or
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Default: None

3.1.12 IPv4MulticastRoute
Property: definitions :: types :: IPv4MulticastRoute
Type: String pattern of ^(23\d|22[4-9])\.((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){2}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)/(23\d|22[4-9])\.((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){2}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)$.

Default: None

3.1.13 IPv4Address
Property: definitions :: types :: IPv4Address
Type: Refer to - definitions->types->DottedQuad
Or
Type: Refer to - definitions->types->IPv4Multicast
Default: None

3.1.14 IPv4MaskReq
Property: definitions :: types :: IPv4MaskReq
Type: Refer to - definitions->types->DottedQuadMaskReq
Or
Type: Refer to - definitions->types->IPv4MulticastMaskReq
Default: None

3.1.15 IPv4MaskOpt
Property: definitions :: types :: IPv4MaskOpt
Type: Refer to - definitions->types->IPv4Address
Or
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

3.1.16 IPv4Route
Property: definitions :: types :: IPv4Route
Type: String.
Type: String pattern of ^((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)/(((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d))$.
Or
Type: Refer to - definitions->types->IPv4MulticastRoute
Default: None

3.1.17 IPv6Address
Property: definitions :: types :: IPv6Address
Type: String pattern of ^((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-

4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?$.
Default: None

3.1.18 IPv6MaskReq

Property: definitions :: types :: IPv6MaskReq
Type: String pattern of ^((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?/(([1][0-2][0-8])|([1-9]\d)|(\d))$.
Default: None

3.1.19 IPv6MaskOpt

Property: definitions :: types :: IPv6MaskOpt
Type: Refer to - definitions->types->IPv6Address
Or
Type: Refer to - definitions->types->IPv6MaskReq
Default: None

3.1.20 IPv6Range

Property: definitions :: types :: IPv6Range
Type: String pattern of ^((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?-((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-

9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?$.
Default: None

3.1.21 IPAddress
Property: definitions :: types :: IPAddress
Type: Refer to - definitions->types->IPv4Address
Or
Type: Refer to - definitions->types->IPv6Address
Default: None

3.1.22 IPAddressMaskReq
Property: definitions :: types :: IPAddressMaskReq
Type: Refer to - definitions->types->IPv4MaskReq
Or
Type: Refer to - definitions->types->IPv6MaskReq
Default: None

3.1.23 IPAddressMaskOpt
Property: definitions :: types :: IPAddressMaskOpt
Type: Refer to - definitions->types->IPv4MaskOpt
Or
Type: Refer to - definitions->types->IPv6MaskOpt
Default: None

3.1.24 IPv4AddressArr
Property: definitions :: types :: IPv4AddressArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPv4Address
Default: None

3.1.25 IPv4MaskReqArr
Property: definitions :: types :: IPv4MaskReqArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPv4MaskReq
Default: None

3.1.26 IPv4MaskOptArr
Property: definitions :: types :: IPv4MaskOptArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPv4MaskOpt
Default: None

3.1.27 IPArrAuto
Property: definitions :: types :: IPArrAuto
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddressMaskOpt
Or
Item type: String enum of auto.
Default: None

3.1.28 IPArrAuto46
Property: definitions :: types :: IPArrAuto46
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddressMaskOpt
Or
Item type: String enum of auto4, auto6.
Default: None

3.1.29 IPArrAutoAll
Property: definitions :: types :: IPArrAutoAll
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddressMaskOpt
Or
Item type: String enum of auto, auto4, auto6.
Default: None

3.1.30 IPv6AddressArr
Property: definitions :: types :: IPv6AddressArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPv6Address
Default: None

3.1.31 IPv6MaskReqArr
Property: definitions :: types :: IPv6MaskReqArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPv6MaskReq
Default: None

3.1.32 IPv6MaskOptArr
Property: definitions :: types :: IPv6MaskOptArr

Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPv6MaskOpt
Default: None

3.1.33 IPAddressRange

Property: definitions :: types :: IPAddressRange
Type: Refer to - definitions->types->DottedQuadRange
Or
Type: Refer to - definitions->types->IPv6Range
Default: None

3.1.34 IPAddressArr

Property: definitions :: types :: IPAddressArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddress
Default: None

3.1.35 IPAddressMaskReqArr

Property: definitions :: types :: IPAddressMaskReqArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddressMaskReq
Default: None

3.1.36 IPAddressMaskOptArr

Property: definitions :: types :: IPAddressMaskOptArr
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->types->IPAddressMaskOpt
Default: None

3.1.37 UINT8

Property: definitions :: types :: UINT8
Type: Integer with a minimum of 0 and a maximum of 255.
Default: None

3.1.38 INT8

Property: definitions :: types :: INT8
Type: Integer with a minimum of -128 and a maximum of 127.
Default: None

3.1.39 UINT16

Property: definitions :: types :: UINT16
Type: Integer with a minimum of 0 and a maximum of 65535.
Default: None

3.1.40 INT16
Property: definitions :: types :: INT16
Type: Integer with a minimum of -32768 and a maximum of 32767.
Default: None

3.1.41 UINT32
Property: definitions :: types :: UINT32
Type: Integer with a minimum of 0 and a maximum of 4294967295.
Default: None

3.1.42 INT32
Property: definitions :: types :: INT32
Type: Integer with a minimum of -2147483648 and a maximum of 2147483647.
Default: None

3.1.43 UINT64
Property: definitions :: types :: UINT64
Type: Integer with a minimum of 0 and a maximum of 18446744073709551615.
Default: None

3.1.44 INT64
Property: definitions :: types :: INT64
Type: Integer with a minimum of -9223372036854775808 and a maximum of 9223372036854775807.
Default: None

3.1.45 VLANIDRange
Property: definitions :: types :: VLANIDRange
Type: Integer with a minimum of 1 and a maximum of 4094.
Default: None

3.1.46 VXLANIDRange
Property: definitions :: types :: VXLANIDRange
Type: Integer with a minimum of 1 and a maximum of 16777215.
Default: None

3.1.47 Port
Property: definitions :: types :: Port
Type: Integer with a minimum of 1 and a maximum of 49151.
Default: None

3.1.48 PortRange
Property: definitions :: types :: PortRange
Type: String with a maximum length of 15 and a pattern of ^([0-9]{1,4}|[1-5][0-9]{4}|6[0-4][0-9]{3}|65[0-4][0-9]{2}|655[0-2][0-9]|6553[0-5])(?:-([0-9]{1,4}|[1-5][0-9]{4}|6[0-4][0-9]{3}|65[0-4][0-9]{2}|655[0-2][0-9]|6553[0-5]))?$.
Default: None

3.1.49 Percentage
Property: definitions :: types :: Percentage
Type: Integer with a minimum of 0 and a maximum of 100.
Default: None

3.1.50 DSCP
Property: definitions :: types :: DSCP
Type: Integer with a minimum of 0 and a maximum of 63.
Default: None

3.1.51 TTL
Property: definitions :: types :: TTL
Type: Integer with a minimum of 1 and a maximum of 255.
Default: None

3.1.52 BooleanInt
Property: definitions :: types :: BooleanInt
Type: Integer with a minimum of 0 and a maximum of 1.
Default: None

3.1.53 File_Dir
Property: definitions :: types :: File_Dir
Type: String pattern of ^[a-zA-Z0-9_/\. \-\\]{2,}$.
Default: None

3.1.54 URI
Property: definitions :: types :: URI
Type: String pattern of ^(([a-zA-Z][a-zA-Z0-9+.-]+):)?(//([^@]+@)?([a-zA-Z0-9.\-_~]+)(:\d+)?)?((?:[a-zA-Z0-9-._~]|%[a-fA-F0-9]|[!$&'()*+,;=:@])+(?:/(?:[a-zA-Z0-9-._~]|%[a-fA-F0-9]|[!$&'()*+,;=:@])*)*|(?:/(?:[a-zA-Z0-9-._~]|%[a-fA-F0-9]|[!$&'()*+,;=:@])+)*)?(\?(?:[a-zA-Z0-9-._~]|%[a-fA-F0-9]|[!$&'()*+,;=:@]|[/?])+)?(\#(?:[a-zA-Z0-9-._~]|%[a-fA-F0-9]|[!$&'()*+,;=:@]|[/?])+)?$.
Default: None

3.1.55 FQDN
Property: definitions :: types :: FQDN

Type: String pattern of (?=^.{2,253}$)(^((?!-)[a-zA-Z0-9-]{0,62}[a-zA-Z0-9]\.)+[a-zA-Z]{2,63}\.?$).
Default: None

3.1.56 FQDN_WC
Property: definitions :: types :: FQDN_WC
Type: String pattern of (?=^.{2,253}$)(^(*\.)+((?!-)[a-zA-Z0-9-]{0,62}[a-zA-Z0-9]\.)*[a-zA-Z]{2,63}\.?$).
Default: None

3.1.57 InterfaceName
Property: definitions :: types :: InterfaceName
Type: String with a minimum length of 1 and a maximum Length of 15 characters and a pattern of ^[a-zA-Z0-9]+([\-_:\.a-zA-Z0-9]+)?$.
Default: None

3.1.58 AlphaNumeric
Property: definitions :: types :: AlphaNumeric
Type: String pattern of ^[a-zA-Z0-9_-]+$.
Default: None

3.2 pki

Property: definitions :: pki
Default: None

3.2.1 file
Property: definitions :: pki :: file
Type: String pattern of ^file://((ecdsa|pkcs8|pkcs12|psks|private|pubkey|rsa|x509|x509ac|x509crl|x509aa|x509ca|x509ocsp)/)?[a-zA-Z0-9_ \.\-]{1,}\.(wpa2|pass|psk|pem|der|cert|crl|crt|csr|cer|pk8|p12|pfx|key|pub|p7b|p7c)$.
Default: None

3.2.2 passphrase_or_wpa2
Property: definitions :: pki :: passphrase_or_wpa2
Type: String pattern of (?!^file://.+)^(.{8,63}|[a-fA-F0-9]{64})$.
Or
Type: String pattern of ^file://((ecdsa|pkcs8|pkcs12|psks|private|pubkey|rsa|x509|x509ac|x509crl|x509aa|x509ca|x509ocsp)/)?[a-zA-Z0-9_ \.\-]+\.wpa2$.
Default: None

3.2.3 password_or_pass

Property: definitions :: pki :: password_or_pass
Type: String pattern of (?!^file://.+)^.{6,}$.
Or
Type: String pattern of ^file://((ecdsa|pkcs8|pkcs12|psks|private|pubkey|rsa|x509|x509ac|x509crl|x509aa|x509ca|x509ocsp)/)?[a-zA-Z0-9_ \.\-]+\.pass$.
Default: None

3.2.4 presharedkey_or_psk

Property: definitions :: pki :: presharedkey_or_psk
Type: String pattern of (?!^file://.+)^[a-zA-Z0-9!@# =\+$%^&*()_\-\?/]{8,130}$.
Or
Type: String pattern of ^file://((ecdsa|pkcs8|pkcs12|psks|private|pubkey|rsa|x509|x509ac|x509crl|x509aa|x509ca|x509ocsp)/)?[a-zA-Z0-9_ \.\-]+\.psk$.
Default: None

3.2.5 ssh_pubkey_or_file

Property: definitions :: pki :: ssh_pubkey_or_file
Type: String pattern of ^(ssh-rsa|ecdsa-sha2-nistp(256|384|521)) (?:[A-Za-z0-9+\/]{4})*(?:[A-Za-z0-9+\/]{2}==|[A-Za-z0-9+\/]{3}=)*(.*)?$.
Or
Type: String pattern of ^file://(pubkey/)?[a-zA-Z0-9_ \.\-]+\.pub$.
Default: None

3.2.6 ssh_key_or_file

Property: definitions :: pki :: ssh_key_or_file
Type: String pattern of ^-----BEGIN OPENSSH PRIVATE KEY-----(.|\n)+-----END OPENSSH PRIVATE KEY-----$.
Or
Type: String pattern of ^file://((rsa|ecdsa|private)/)?[a-zA-Z0-9_ \.\-]+(\.key)?$.
Default: None

3.2.7 ssh_keypair

Property: definitions :: pki :: ssh_keypair
Type: JSON Object
Required: ['Name', 'PublicKey', 'PrivateKey']
Default: None

3.2.7.1 Name

Property: definitions :: pki :: ssh_keypair :: Name
Type: Refer to - definitions->types->AlphaNumeric
Default: None

3.2.7.2 PublicKey
Property: definitions :: pki :: ssh_keypair :: PublicKey
Type: Refer to - definitions->pki->ssh_pubkey_or_file
Default: None

3.2.7.3 PrivateKey
Property: definitions :: pki :: ssh_keypair :: PrivateKey
Type: Refer to - definitions->pki->ssh_key_or_file
Default: None

3.3 logging

Property: definitions :: logging
Default: None

3.3.1 LogVerbosity
Property: definitions :: logging :: LogVerbosity
Type: String enum of critical, error, warning, notice, info, debug, uber.
Default: None

3.3.2 LogBuckets
Property: definitions :: logging :: LogBuckets
Type: String enum of general, packet, packeticmp, packetigmp, packetunicast, packetmulticast, packetudp, packettcp, packetme, tunnel, neighbor, frr, frrospf, frrpim, frrstatic, frrzebra, link, linktable, linkstate, linkquality, ipc, ipclink, ipcoption, ipcpolicy, ipcpacket, aresh, system, plugin, wlanmanager, vpn, flowredirector, freeboard, mantra, mre, radiocontroller, reconfiguration, visualizer, tscanr, bit, zoom, zoomclient, dhcp, find.
Default: None

3.4 tunnel

Property: definitions :: tunnel
Default: None

3.4.1 EncapType
Property: definitions :: tunnel :: EncapType
Type: String enum of fou, gue.
Default: None

3.5 bonding

Property: definitions :: bonding

Default: None

3.5.1 ADSelect
Property: definitions :: bonding :: ADSelect
Type: String enum of stable, bandwidth, count.
Default: None

3.5.2 ARPValidate
Property: definitions :: bonding :: ARPValidate
Type: String enum of none, active, backup, all, filter, filter-active, filter-backup.
Default: None

3.5.3 PrimaryReselect
Property: definitions :: bonding :: PrimaryReselect
Type: String enum of always, better, failure.
Default: None

3.5.4 FailoverMAC
Property: definitions :: bonding :: FailoverMAC
Type: String enum of none, active, follow.
Default: None

3.5.5 LACP
Property: definitions :: bonding :: LACP
Type: String enum of slow, fast.
Default: None

3.5.6 XmitHashPolicy
Property: definitions :: bonding :: XmitHashPolicy
Type: String enum of layer2, layer2+3, layer3+4, encap2+3, encap3+4.
Default: None

3.5.7 Modes
Property: definitions :: bonding :: Modes
Type: String enum of balance-rr, active-backup, balance-xor, broadcast, 802.3ad, balance-tlb, balance-alb.
Default: None

3.6 staticroutes

Property: definitions :: staticroutes
Default: None

3.6.1 RouteObject

Property: definitions :: staticroutes :: RouteObject
Description: IPv4 or IPv6 Route information. Subnet and Via address versions must match.
Type: JSON Object
Required: ['Network']
Default: None

3.6.1.1 Network

Property: definitions :: staticroutes :: RouteObject :: Network
Description: The IPv4 or IPv6 subnet that is reachable.
Type: Refer to - definitions->types->IPAddressMaskReq
Or
Type: String enum of default4, default6.
Default: None

3.6.1.2 Via

Property: definitions :: staticroutes :: RouteObject :: Via
Description: The IPv4 or IPv6 gateway address used to reach the subnet.
Type: Refer to - definitions->types->IPAddress
Default: None

3.6.1.3 Metric

Property: definitions :: staticroutes :: RouteObject :: Metric
Description: The metric set on the route.
Type: Integer with a minimum of 1 and a maximum of 255.
Default: 1

3.6.1.4 Nexthop-VRF

Property: definitions :: staticroutes :: RouteObject :: Nexthop-VRF
Description: Create a leaked route with a next hop in the specified VRF
Type: Refer to - definitions->types->InterfaceName
Default: None

3.6.1.5 Advertise

Property: definitions :: staticroutes :: RouteObject :: Advertise
Description: Advertise this route over OSPF. Only happens if one or more links have OSPF enabled.
Type: Boolean true or false.
Default: False

3.7 ospf

Property: definitions :: ospf
Default: None

3.7.1 ABRTypes
Property: definitions :: ospf :: ABRTypes
Type: String enum of cisco, ibm, standard, shortcut.
Default: None

3.7.2 OSPFArea
Property: definitions :: ospf :: OSPFArea
Type: Refer to - definitions->types->UINT32
Or
Type: Refer to - definitions->types->DottedQuad
Default: None

3.7.3 OSPFAuthentication
Property: definitions :: ospf :: OSPFAuthentication
Type: JSON Object
Required: ['Type', 'Password']
Default: None

3.7.3.1 Type
Property: definitions :: ospf :: OSPFAuthentication :: Type
Description: Simple password authentication for OSPF.
Type: String enum of password.
Default: None

3.7.3.2 Password
Property: definitions :: ospf :: OSPFAuthentication :: Password
Description: The password used for authentication.
Type: String with a minimum length of 1 and a maximum Length of 8 characters.
Or
Required: ['Type', 'KeyId', 'Key']
Default: None

3.7.3.3 Type
Property: definitions :: ospf :: OSPFAuthentication :: Type
Description: Digest authentication type that uses a cryptographic password. The cryptographic algorithm is MD5.
Type: String enum of digest.
Default: None

3.7.3.4 KeyId
Property: definitions :: ospf :: OSPFAuthentication :: KeyId

Description: The secret key used to create the message digest. This ID is part of the protocol and must be consistent across routers on the link.
Type: Integer with a minimum of 1 and a maximum of 255.
Default: None

3.7.3.5 Key
Property: definitions :: ospf :: OSPFAuthentication :: Key
Description: The actual message digest key.
Type: String with a minimum length of 1 and a maximum Length of 16 characters.
Default: None

3.7.4 wlanmanager
Property: definitions :: wlanmanager
Default: None

3.7.5 wifi_ssid
Property: definitions :: wlanmanager :: wifi_ssid
Type: String with a minimum length of 1 and a maximum Length of 32 characters.
Default: None

3.7.6 802.11Protocols
Property: definitions :: wlanmanager :: 802.11Protocols
Type: Array of unique items and a minimum number of 1 item(s).
Item type: String enum of 802.11a, 802.11b, 802.11g, 802.11n_2.4g, 802.11n_5g, 802.11ac.
Default: None

3.7.7 channel
Property: definitions :: wlanmanager :: channel
Type: Enum of 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 25, 26, 27, 29, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 46, 48, 49, 50, 52, 53, 54, 56, 57, 58, 60, 61, 62, 64, 65, 68, 69, 73, 77, 81, 85, 89, 93, 96, 97, 100, 101, 102, 104, 105, 106, 108, 109, 110, 112, 113, 114, 116, 117, 118, 120, 121, 122, 124, 125, 126, 128, 129, 131, 132, 133, 134, 135, 136, 137, 138, 140, 141, 142, 144, 145, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 180, 181, 182, 183, 184, 185, 187, 188, 189, 192, 193, 196, 197, 201, 205, 209, 213, 217, 221, 225, 229, 233.
Default: None

3.7.8 channelorauto
Property: definitions :: wlanmanager :: channelorauto
Type: Refer to - definitions->wlanmanager->channel
Or
Type: Enum of auto.
Default: None

3.8 vpn

Property: definitions :: vpn
Default: None

3.8.1 SmartCard

Property: definitions :: vpn :: SmartCard
Type: String pattern of ^(%smartcard((\d{1,10}){1}(@[a-zA-Z]{1,255})?)?:(\d{1,10}))$.
Default: None

3.8.2 IPProtoPortArrAuto

Property: definitions :: vpn :: IPProtoPortArrAuto
Description: An array of IPsec subnet definitions, or the keyword 'auto'. IPsec subnet definitions follow the format <ip subnet>[[<proto/port>]][,...]. The keyword '%any' can be used in place of a specific proto or port definition and is assumed if none is given. Ex. '10.0.0.0/8[tcp/%any]'
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->vpn->IPSecSubnet
Or
Item type: String enum of auto.
Default: None

3.8.3 IPSecSubnet

Property: definitions :: vpn :: IPSecSubnet
Type: String pattern of ^(((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\/(3[0-2]|[1-2]?\d))?|((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?(\/(([1][0-2][0-8])|([1-9]\d)|(\d)))?)(\[(udp|tcp|%any|(25[0-5]|2[0-4]\d|1\d\d|[1-9]\d|\d))?(\/(6553[0-5]|655[0-2]\d|65[0-4]\d\d|6[0-4]\d\d\d|[1-5]\d\d\d\d|[1-9]\d\d\d|[1-9]\d\d|[1-9]?\d|%any))?\])?$.
Default: None

3.8.4 AuthRound

Property: definitions :: vpn :: AuthRound
Description: Section for a single authentication round, defining the rules for how authentication is performed for the local peers or for how peers must authenticate to use this connection.
Type: JSON Object

Default: None

r**ound**
Property: definitions :: vpn :: AuthRound :: round
Description: Optional numeric identifier by which authentication rounds are sorted. If not specified, rounds are ordered by their position in the config file or vici message.
Type: Integer with a minimum of 0 and a maximum of 63.
Default: None

3.8.4.1 auth
Property: definitions :: vpn :: AuthRound :: auth
Description: Authentication to perform locally or accept from remote.
pubkey - Use public key authentication based on a private key associated with a useable certificate.
psk - Use pre-shared key authentication
xauth - Use XAuth or Hybrid authentication (IKEv1); a specific backend name may be appended, separated by a dash
eap - Use EAP authentication (IKEv2); a specific EAP method name may be appended, separated by a dash
If both peers support IKEv2 Signature Authentication (RFC 7427), specific hash algorithms to be used during IKEv2 authentication may be configured. To do so, use ike: followed by a trust chain signature scheme constraint.
Type: String pattern of ^(ike:)?(pubkey|psk|never|eap|xauth(-(eap|noauth|pam))?|eap-aka|eap-gtc|eap-mschapv2|eap-peap|eap-tls|eap-ttls|eap-dynamic|eap-radius|rsa|ecdsa|rsa-ecdsa|rsa-2048|ecdsa-256|rsa-2048-ecdsa-256|rsa-2048-sha256-sha384-sha512|ecdsa-256-sha256-sha384-sha512)$.
Default: pubkey

3.8.4.2 id
Property: definitions :: vpn :: AuthRound :: id
Description: IKE identity to use or expect for authentication round. When using certificate authentication, the IKE identity must be contained in the certificate, either as the subject DN or as a subjectAltName (will default to subject DN if not specified). Wildcards (*) may be used to match remote identities.
Type: String.
Default: None

3.8.4.3 eap_id
Property: definitions :: vpn :: AuthRound :: eap_id
Description: EAP-Identity to use in EAP-Identity exchange and the EAP method.
Type: String.
Default: None

3.8.4.4 certs

Property: definitions :: vpn :: AuthRound :: certs
Description: List of certificates to use or accept for authentication.
Type: Array of unique items.
Type: Refer to - definitions->pki->file
Default: None

3.8.4.5 pubkeys
Property: definitions :: vpn :: AuthRound :: pubkeys
Description: List of raw public keys to use or accept for authentication. Even though multiple local public keys can be defined, only the first public key in the list is used for authentication.
Type: Array of unique items.
Type: Refer to - definitions->pki->file
Default: None

3.8.4.6 AuthRound :: <pattern>
Property: definitions :: vpn :: AuthRound :: ^(?!certs)cert[a-zA-Z0-9_-]{0,20}$
Type: Refer to - definitions->vpn->SingleCert
Default: None

3.8.5 SingleCert
Property: definitions :: vpn :: SingleCert
Description: A single cert subsection for a certificate to use or accept for authentication. Certificates in certs/cacerts are transmitted as binary blobs whereas the subsections offer more flexibility.
Type: JSON Object
Required: ['file']
Or
Required: ['handle']
Default: None

3.8.5.1 file
Property: definitions :: vpn :: SingleCert :: file
Description: The certificate file.
Type: Refer to - definitions->pki->file
Default: None

3.8.5.2 handle
Property: definitions :: vpn :: SingleCert :: handle
Description: Hex-encoded CKA_ID or handle of the certificate on a token or TPM 2.0, respectively.
Type: String pattern of ^[a-fA-F0-9]+$.
Default: None

3.8.5.3 slot

Property: definitions :: vpn :: SingleCert :: slot
Description: Optional slot number of the token that stores the certificate.
Type: Integer with a minimum of 0.
Default: None

3.8.5.4 module
Property: definitions :: vpn :: SingleCert :: module
Description: Optional PKCS#11 module name.
Type: String.
Default: None

3.8.6 NetfilterMarkMask
Property: definitions :: vpn :: NetfilterMarkMask
Type: String pattern of ^([0-9]|[1-9][0-9]{1,8}|[1-3][0-9]{9}|4[01][0-9]{8}|42[0-8][0-9]{7}|429[0-3][0-9]{6}|4294[0-8][0-9]{5}|42949[0-5][0-9]{4}|429496[0-6][0-9]{3}|4294967[01][0-9]{2}|42949672[0-8][0-9]|429496729[0-5])(\/0x[a-f0-9]{1,8})?$.
Default: None

3.8.7 if_id
Property: definitions :: vpn :: if_id
Type: Refer to - definitions->types->UINT32
Or
Type: String enum of %unique, %unique-dir.
Default: None

3.8.8 NIAPAEADProposal
Property: definitions :: vpn :: NIAPAEADProposal
Description: Authenticated Encryption with Associated Data (AEAD) algorithms can't be combined with classic encryption ciphers in the same proposal. No separate integrity algorithm must be proposed and therefore Pseudo-Random Functions (PRFs) have to be included explicitly in such proposals.
Type: JSON Object
Required: ['aead_algorithms', 'pseudo_random_functions', 'ke_groups']
Default: None

3.8.8.1 aead_algorithms
Property: definitions :: vpn :: NIAPAEADProposal :: aead_algorithms
Type: Refer to - definitions->vpn->niap_aead_algorithms
Default: None

3.8.8.2 pseudo_random_functions
Property: definitions :: vpn :: NIAPAEADProposal :: pseudo_random_functions
Type: Refer to - definitions->vpn->niap_pseudo_random_functions
Default: None

3.8.8.3 ke_groups
Property: definitions :: vpn :: NIAPAEADProposal :: ke_groups
Type: Refer to - definitions->vpn->niap_ke_groups
Default: None

3.8.9 NIAPNonAEADProposal
Property: definitions :: vpn :: NIAPNonAEADProposal
Description: A non-AEAD proposal consisting of an encryption algorithm, an integrity algorithm, an optional pseudo-random function, and a Diffie-Hellman key exchange group
Type: JSON Object
Required: ['encryption_algorithms', 'integrity_algorithms', 'ke_groups']
Default: None

3.8.9.1 encryption_algorithms
Property: definitions :: vpn :: NIAPNonAEADProposal :: encryption_algorithms
Type: Refer to - definitions->vpn->niap_encryption_algorithms
Default: None

3.8.9.2 integrity_algorithms
Property: definitions :: vpn :: NIAPNonAEADProposal :: integrity_algorithms
Type: Refer to - definitions->vpn->niap_integrity_algorithms
Default: None

3.8.9.3 pseudo_random_functions
Property: definitions :: vpn :: NIAPNonAEADProposal :: pseudo_random_functions
Type: Refer to - definitions->vpn->niap_pseudo_random_functions
Default: None

3.8.9.4 ke_groups
Property: definitions :: vpn :: NIAPNonAEADProposal :: ke_groups
Type: Refer to - definitions->vpn->niap_ke_groups
Default: None

3.8.10 NIAPAHProposal
Property: definitions :: vpn :: NIAPAHProposal
Description: Authentication Header (AH) proposals (sets of algorithms) to offer for the CHILD_SA. Consist of integrity algorithm(s) and optional Diffie-Hellman key exchange group(s).
Type: JSON Object
Required: ['integrity_algorithms']
Default: None

3.8.10.1 integrity_algorithms
Property: definitions :: vpn :: NIAPAHProposal :: integrity_algorithms
Type: Refer to - definitions->vpn->niap_integrity_algorithms
Default: None

3.8.10.2 ke_groups
Property: definitions :: vpn :: NIAPAHProposal :: ke_groups
Type: Refer to - definitions->vpn->niap_ke_groups
Default: None

3.8.10.3 esn_mode
Property: definitions :: vpn :: NIAPAHProposal :: esn_mode
Description: Extended Sequence Number support may be indicated with the esn and noesn values. Both may be included to indicate support for both modes. If omitted, noesn is assumed.
Type: String enum of esn, noesn, esn-noesn.
Default: noesn

3.8.11 NIAPESPProposal
Property: definitions :: vpn :: NIAPESPProposal
Description: Encapsulating Security Payload (ESP) proposals (sets of algorithms) to offer for the CHILD_SA.
Non-AEAD proposals: encryption algorithm, integrity algorithm, optional Diffie-Hellman group, optional Extended Sequence Number Mode (ESN) indicator.
Type: JSON Object
Required: ['encryption_algorithms', 'integrity_algorithms']
Default: None

3.8.11.1 esn_mode
Property: definitions :: vpn :: NIAPESPProposal :: esn_mode
Description: Extended Sequence Number support may be indicated with the esn and noesn values. Both may be included to indicate support for both modes. If omitted, noesn is assumed.
Type: String enum of esn, noesn, esn-noesn.
Default: noesn

3.8.12 ke_groups
Property: definitions :: vpn :: NIAPESPProposal :: ke_groups
Type: Refer to - definitions->vpn->niap_ke_groups
Default: None

3.8.13 encryption_algorithms
Property: definitions :: vpn :: NIAPESPProposal :: encryption_algorithms
Type: Refer to - definitions->vpn->niap_encryption_algorithms
Default: None

3.8.14 integrity_algorithms
Property: definitions :: vpn :: NIAPESPProposal :: integrity_algorithms
Type: Refer to - definitions->vpn->niap_integrity_algorithms
Default: None

3.8.15 niap_encryption_algorithms
Property: definitions :: vpn :: niap_encryption_algorithms
Description: Encryption algorithms
Type: Array with a minimum number of 1 item(s).
Item type: String enum of aes128, aes256.
Default: None

3.8.16 niap_integrity_algorithms
Property: definitions :: vpn :: niap_integrity_algorithms
Description: Integrity algorithms
Type: Array with a minimum number of 1 item(s).
Item type: String enum of sha256, sha384, sha512.
Default: None

3.8.17 niap_aead_algorithms
Property: definitions :: vpn :: niap_aead_algorithms
Description: Authenticated Encryption with Associated Data (AEAD) algorithms
Type: Array with a minimum number of 1 item(s).
Item type: String enum of aes128gcm8, aes256gcm8, aes128gcm12, aes256gcm12, aes128gcm16, aes256gcm16.
Default: None

3.8.18 niap_pseudo_random_functions
Property: definitions :: vpn :: niap_pseudo_random_functions
Description: Pseudo-random functions
Type: Array with a minimum number of 1 item(s).
Item type: String enum of prfsha256, prfsha384, prfsha512.
Default: None

3.8.19 niap_ke_groups
Property: definitions :: vpn :: niap_ke_groups
Description: Diffie-Hellman key exchange groups
Type: Array with a minimum number of 1 item(s).
Item type: String enum of modp2048, modp2048s256, ecp256, ecp384.
Default: None

3.8.20 AEADProposal
Property: definitions :: vpn :: AEADProposal

Description: Authenticated Encryption with Associated Data (AEAD) algorithms can't be combined with classic encryption ciphers in the same proposal. No separate integrity algorithm must be proposed and therefore Pseudo-Random Functions (PRFs) have to be included explicitly in such proposals.
Type: JSON Object
Required: ['aead_algorithms', 'pseudo_random_functions', 'ke_groups']
Default: None

3.8.20.1 aead_algorithms
Property: definitions :: vpn :: AEADProposal :: aead_algorithms
Type: Refer to - definitions->vpn->aead_algorithms
Default: None

3.8.20.2 pseudo_random_functions
Property: definitions :: vpn :: AEADProposal :: pseudo_random_functions
Type: Refer to - definitions->vpn->pseudo_random_functions
Default: None

3.8.20.3 ke_groups
Property: definitions :: vpn :: AEADProposal :: ke_groups
Type: Refer to - definitions->vpn->ke_groups
Default: None

3.8.21 NonAEADProposal
Property: definitions :: vpn :: NonAEADProposal
Description: A non-AEAD proposal consisting of an encryption algorithm, an integrity algorithm, an optional pseudo-random function, and a Diffie-Hellman key exchange group
Type: JSON Object
Required: ['encryption_algorithms', 'integrity_algorithms', 'ke_groups']
Default: None

3.8.21.1 encryption_algorithms
Property: definitions :: vpn :: NonAEADProposal :: encryption_algorithms
Type: Refer to - definitions->vpn->encryption_algorithms
Default: None

3.8.21.2 integrity_algorithms
Property: definitions :: vpn :: NonAEADProposal :: integrity_algorithms
Type: Refer to - definitions->vpn->integrity_algorithms
Default: None

3.8.21.3 pseudo_random_functions
Property: definitions :: vpn :: NonAEADProposal :: pseudo_random_functions

Type: Refer to - definitions->vpn->pseudo_random_functions
Default: None

3.8.21.4 ke_groups
Property: definitions :: vpn :: NonAEADProposal :: ke_groups
Type: Refer to - definitions->vpn->ke_groups
Default: None

3.8.22 AHProposal
Property: definitions :: vpn :: AHProposal
Description: Authentication Header (AH) proposals (sets of algorithms) to offer for the CHILD_SA. Consist of integrity algorithm(s) and optional Diffie-Hellman key exchange group(s).
Type: JSON Object
Required: ['integrity_algorithms']
Default: None

3.8.22.1 integrity_algorithms
Property: definitions :: vpn :: AHProposal :: integrity_algorithms
Type: Refer to - definitions->vpn->integrity_algorithms
Default: None

3.8.22.2 ke_groups
Property: definitions :: vpn :: AHProposal :: ke_groups
Type: Refer to - definitions->vpn->ke_groups
Default: None

3.8.22.3 esn_mode
Property: definitions :: vpn :: AHProposal :: esn_mode
Description: Extended Sequence Number support may be indicated with the esn and noesn values. Both may be included to indicate support for both modes. If omitted, noesn is assumed.
Type: String enum of esn, noesn, esn-noesn.
Default: noesn

3.8.23 ESPProposal
Property: definitions :: vpn :: ESPProposal
Description: Encapsulating Security Payload (ESP) proposals (sets of algorithms) to offer for the CHILD_SA.
Non-AEAD proposals: encryption algorithm, integrity algorithm, optional Diffie-Hellman group, optional Extended Sequence Number Mode (ESN) indicator.
AEAD proposals: combined mode algorithm, optional Diffie-Hellman group, optional ESN indicator.
Type: JSON Object
Default: None

3.8.23.1 esn_mode
Property: definitions :: vpn :: ESPProposal :: esn_mode
Description: Extended Sequence Number support may be indicated with the esn and noesn values. Both may be included to indicate support for both modes. If omitted, noesn is assumed.
Type: String enum of esn, noesn, esn-noesn.
Default: noesn

3.8.23.2 ke_groups
Property: definitions :: vpn :: ESPProposal :: ke_groups
Type: Refer to - definitions->vpn->ke_groups
And
Description: A proposal consisting of Authenticated Encryption with Associated Data (AEAD) algorithms (providing combined encryption and integrity) and optional Diffie-Hellman key exchange groups.
Type: JSON Object
Required: ['aead_algorithms']
Default: None

3.8.23.3 aead_algorithms
Property: definitions :: vpn :: ESPProposal :: aead_algorithms
Type: Refer to - definitions->vpn->aead_algorithms
esn_mode: True
ke_groups: True
Or
Description: A non-AEAD proposal consisting of an encryption algorithm, an integrity algorithm, and an optional Diffie-Hellman key exchange group.
Type: JSON Object
Required: ['encryption_algorithms', 'integrity_algorithms']
Default: None

3.8.23.4 encryption_algorithms
Property: definitions :: vpn :: ESPProposal :: encryption_algorithms
Type: Refer to - definitions->vpn->encryption_algorithms
Default: None

3.8.23.5 integrity_algorithms
Property: definitions :: vpn :: ESPProposal :: integrity_algorithms
Type: Refer to - definitions->vpn->integrity_algorithms
esn_mode: True
ke_groups: True
Default: None

3.8.24 encryption_algorithms

Property: definitions :: vpn :: encryption_algorithms
Description: Encryption algorithms
Type: Array with a minimum number of 1 item(s).
Item type: String enum of des, 3des, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256, camellia128ctr, camellia192ctr, camellia256ctr, cast128, blowfish128, blowfish192, blowfish256, null, serpent128, serpent192, serpent256, twofish128, twofish192, twofish256.
Default: None

3.8.25 integrity_algorithms

Property: definitions :: vpn :: integrity_algorithms
Description: Integrity algorithms
Type: Array with a minimum number of 1 item(s).
Item type: String enum of aescmac, aesxcbc, camelliaxcbc, md5, md5_128, sha1, sha1_160, sha256, sha384, sha512, sha256_96.
Default: None

3.8.26 aead_algorithms

Property: definitions :: vpn :: aead_algorithms
Description: Authenticated Encryption with Associated Data (AEAD) algorithms
Type: Array with a minimum number of 1 item(s).
Item type: String enum of aes128ccm8, aes192ccm8, aes256ccm8, aes128ccm12, aes192ccm12, aes256ccm12, aes128ccm16, aes192ccm16, aes256ccm16, aes128gcm8, aes192gcm8, aes256gcm8, aes128gcm12, aes192gcm12, aes256gcm12, aes128gcm16, aes192gcm16, aes256gcm16, camellia128ccm8, camellia192ccm8, camellia256ccm8, camellia128ccm12, camellia192ccm12, camellia256ccm12, camellia128ccm16, camellia192ccm16, camellia256ccm16, chacha20poly1305.
Default: None

3.8.27 pseudo_random_functions

Property: definitions :: vpn :: pseudo_random_functions
Description: Pseudo-random functions
Type: Array with a minimum number of 1 item(s).
Item type: String enum of prfmd5, prfsha1, prfaesxcbc, prfaescmac, prfsha256, prfsha384, prfsha512, prfcamelliaxcbc.
Default: None

3.8.28 ke_groups

Property: definitions :: vpn :: ke_groups
Description: Diffie-Hellman key exchange groups
Type: Array with a minimum number of 1 item(s).
Item type: String enum of modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, modp1024s160, modp2048s224, modp2048s256, ecp192, ecp224,

ecp256, ecp384, ecp521, ecp224bp, ecp256bp, ecp384bp, ecp512bp, curve25519, curve448, frodos1, frodos3, frodos5, frodoa1, frodoa3, frodoa5.
Default: None

3.8.29 children_base
Property: definitions :: vpn :: children_base
Description: A single CHILD_SA configuration.
Type: JSON Object
Default: None

3.8.29.1 References
Property: definitions :: vpn :: children_base :: References
Description: List of default child sections that will be inherited into this child.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^[a-zA-Z0-9_-\.]+$.
Default: None

3.8.29.2 firewall
Property: definitions :: vpn :: children_base :: firewall
Description: When enabled, automatically add/remove rules to allow VPN traffic through the firewall
Type: Boolean true or false.
Default: False
ah_proposals: True
esp_proposals: True
Default: None

3.8.29.3 sha256_96
Property: definitions :: vpn :: children_base :: sha256_96
Description: HMAC-SHA-256 is used with 128-bit truncation with IPsec. For compatibility with implementations that incorrectly use 96-bit truncation this option may be enabled to configure the shorter truncation length in the kernel. Not negotiated, peer must use the incorrect length or set this option as well.
Type: Boolean true or false.
Default: False

3.8.29.4 local_ts
Property: definitions :: vpn :: children_base :: local_ts
Description: List of local traffic selectors to include in CHILD_SA. Each selector is a CIDR subnet definition, followed by an optional proto/port selector (<subnet>[proto/port]). The special value dynamic may be used instead of a subnet definition, which gets replaced by the tunnel outer address or the virtual IP if negotiated. When IKEv1 is used, only the first selector is interpreted, but multiple CHILD_SAs with different selectors may be defined.
Type: Array of unique items.

Item type: String pattern of ^(dynamic|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\/(3[0-2]|[1-2]?\d))?|((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?(\/(([1][0-2][0-8])|([1-9]\d)|(\d)))?)(\[(udp|tcp|%any|(25[0-5]|2[0-4]\d|1\d\d|[1-9]\d|\d))?(\/[!-~]{1,50})?\])?$.
Default: ['dynamic']

3.8.29.5 remote_ts

Property: definitions :: vpn :: children_base :: remote_ts
Description: List of remote traffic selectors to include in CHILD_SA.
Type: Array of unique items.
Item type: String pattern of ^(dynamic|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\/(3[0-2]|[1-2]?\d))?|((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?(\/(([1][0-2][0-8])|([1-9]\d)|(\d)))?)(\[(udp|tcp|%any|(25[0-5]|2[0-4]\d|1\d\d|[1-9]\d|\d))?(\/[!-~]{1,50})?\])?$.
Default: ['dynamic']

3.8.29.6 rekey_time

Property: definitions :: vpn :: children_base :: rekey_time
Description: Time to schedule CHILD_SA rekeying. CHILD_SA rekeying refreshes key material, optionally using a Diffie-Hellman exchange if a group is specified in the proposal.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: 1h

3.8.29.7 life_time

Property: definitions :: vpn :: children_base :: life_time

Description: Maximum lifetime before CHILD_SA gets closed (if rekeying fails). Default is 10% more than rekey_time.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: None

3.8.29.8 rand_time

Property: definitions :: vpn :: children_base :: rand_time
Description: Time range from which to choose a random value to subtract from rekey_time. Default is the difference between life_time and rekey_time.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: None

3.8.29.9 rekey_bytes

Property: definitions :: vpn :: children_base :: rekey_bytes
Description: Number of bytes processed before initiating CHILD_SA rekeying. Volume based CHILD_SA rekeying is disabled by default.
Type: Integer with a minimum of 10000000 and a maximum of 4000000000.
Default: None

3.8.29.10 life_bytes

Property: definitions :: vpn :: children_base :: life_bytes
Description: Maximum bytes processed before CHILD_SA gets closed. Default is 10% more than rekey_bytes.
Type: Integer with a minimum of 10000000 and a maximum of 4000000000.
Default: None

3.8.29.11 rand_bytes

Property: definitions :: vpn :: children_base :: rand_bytes
Description: Byte range from which to choose a random value to subtract from rekey_bytes. Default is difference between life_bytes and rekey_bytes.
Type: Integer with a minimum of 1000000 and a maximum of 10000000.
Default: None

3.8.29.12 rekey_packets

Property: definitions :: vpn :: children_base :: rekey_packets
Description: Number of packets processed before initiating CHILD_SA rekeying. Packet count based CHILD_SA rekeying is disabled by default.
Type: Integer with a minimum of 10000000 and a maximum of 4000000000.
Default: None

3.8.29.13 life_packets

Property: definitions :: vpn :: children_base :: life_packets
Description: Maximum number of packets processed before CHILD_SA gets closed. Default is 10% more than rekey_packets.

Type: Integer with a minimum of 10000000 and a maximum of 4000000000.
Default: None

3.8.29.14 rand_packets

Property: definitions :: vpn :: children_base :: rand_packets
Description: Packet range from which to choose a random value to subtract from rekey_packets. Default is difference between life_packets and rekey_packets.
Type: Integer with a minimum of 1000000 and a maximum of 10000000.
Default: None

3.8.29.15 hostaccess

Property: definitions :: vpn :: children_base :: hostaccess
Description: Pass host access variable to updown script.
Type: Boolean true or false.
Default: False

3.8.29.16 mode

Property: definitions :: vpn :: children_base :: mode
Description: IPsec mode to establish CHILD_SA with:
tunnel - Host-to-Host, Host-to-Subnet, or Subnet-to-Subnet tunnel mode
transport - Host-to-Host transport mode
transport_proxy - Special Mobile IPv6 transport proxy mode
beet - Bound End to End Tunnel mixture mode, uses fixed inner addresses without the need to include them in each packet
pass - No IPsec processing, packets are passed as-is
drop - Packets are discarded
Type: String enum of tunnel, transport, transport_proxy, beet, pass, drop.
Default: tunnel

3.8.29.17 policies

Property: definitions :: vpn :: children_base :: policies
Description: Whether to install IPsec policies or not.
Type: Boolean true or false.
Default: True

3.8.29.18 policies_fwd_out

Property: definitions :: vpn :: children_base :: policies_fwd_out
Description: Whether to install outbound FWD IPsec policies or not.
Type: Boolean true or false.
Default: False

3.8.29.19 dpd_action

Property: definitions :: vpn :: children_base :: dpd_action
Description: The action to perform for this CHILD_SA on DPD (Dead Peer Detection) timeout.

clear - The connection is closed with no further actions taken.
trap - Trap policy is installed, which will catch matching traffic and try to re-negotiate the connection on demand.
restart - Immediately triggers an attempt to re-negotiate the connection.
Type: String enum of clear, trap, restart.
Default: clear

3.8.29.20 ipcomp

Property: definitions :: vpn :: children_base :: ipcomp
Description: Enable IPComp compression before encryption.
Type: Boolean true or false.
Default: False

3.8.29.21 inactivity

Property: definitions :: vpn :: children_base :: inactivity
Description: Timeout before closing CHILD_SA after inactivity. Default value of 0 disables inactivity checks.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: 0s

3.8.29.22 reqid

Property: definitions :: vpn :: children_base :: reqid
Description: Fixed reqid to use for this CHILD_SA. Works only if each CHILD_SA configuration is instantiated not more than once. Default value of 0 uses dynamic reqids, allocated incrementally.
Type: Integer with a minimum of 0.
Default: 0

3.8.29.23 priority

Property: definitions :: vpn :: children_base :: priority
Description: Optional fixed priority for IPsec policies. This could be useful to install high-priority drop policies. The default of 0 uses dynamically calculated priorities based on the size of the traffic selectors.
Type: Integer with a minimum of 0.
Default: 0

3.8.29.24 interface

Property: definitions :: vpn :: children_base :: interface
Description: Optional interface name to restrict outbound IPsec policies to.
Type: Refer to - definitions->types->InterfaceName
Default: None

3.8.29.25 mark_in

Property: definitions :: vpn :: children_base :: mark_in

Description: Netfilter mark and mask for input traffic. The special value %unique sets a unique mark on each CHILD_SA instance. The special value %unique-dir assigns a different unique mark for each CHILD_SA direction (in/out). An additional mask may be appended to the mark separated by /.
Type: Enum of %unique, %unique-dir.
Or
Type: Refer to - definitions->vpn->NetfilterMarkMask
Default: None

3.8.29.26 mark_in_sa

Property: definitions :: vpn :: children_base :: mark_in_sa
Description: Whether to set mark_in on the inbound SA. By default, the inbound mark is only set on the inbound policy.
Type: Boolean true or false.
Default: False

3.8.29.27 mark_out

Property: definitions :: vpn :: children_base :: mark_out
Description: Netfilter mark and mask for output traffic. The special value %unique sets a unique mark on each CHILD_SA instance. The special value %unique-dir assigns a different unique mark for each CHILD_SA direction (in/out). An additional mask may be appended to the mark separated by /.
Type: Enum of %unique, %unique-dir.
Or
Type: Refer to - definitions->vpn->NetfilterMarkMask
Default: None

3.8.29.28 set_mark_in

Property: definitions :: vpn :: children_base :: set_mark_in
Description: Netfilter mark applied to packets after the inbound IPsec SA processed them. An additional mask may be appended to the mark separated by /. The special value %same uses the value (but not the mask) from mark_in.
Type: Enum of %same.
Or
Type: Refer to - definitions->vpn->NetfilterMarkMask
Default: None

3.8.29.29 set_mark_out

Property: definitions :: vpn :: children_base :: set_mark_out
Description: Netfilter mark applied to packets after the outbound IPsec SA processed them. An additional mask may be appended to the mark separated by /. The special value %same uses the value (but not the mask) from mark_out.
Type: Enum of %same.
Or

Type: Refer to - definitions->vpn->NetfilterMarkMask
Default: None

3.8.29.30 if_id_in

Property: definitions :: vpn :: children_base :: if_id_in
Description: XFRM interface ID set on in-bound policies/SA.
The special value %unique sets a unique interface ID on each CHILD_SA instance.
The special value %unique-dir assigns a different unique interface ID for each CHILD_SA direction (in/out).
Type: Refer to - definitions->vpn->if_id
Default: 0

3.8.29.31 if_id_out

Property: definitions :: vpn :: children_base :: if_id_out
Description: XFRM interface ID set on out-bound policies/SA.
The special value %unique sets a unique interface ID on each CHILD_SA instance.
The special value %unique-dir assigns a different unique interface ID for each CHILD_SA direction (in/out).
Type: Refer to - definitions->vpn->if_id
Default: 0

3.8.29.32 label

Property: definitions :: vpn :: children_base :: label
Description: Optional security label (e.g. SELinux content), IKEv2 only.
Type: String.
Default: None

3.8.29.33 label_mode

Property: definitions :: vpn :: children_base :: label_mode
Description: Defines the mode in which the configured security label is used. The default value of system selects selinux if strongSwan was built with SELinux support and SELinux is enabled by the kernel, otherwise simple will be selected.
simple - The label will be used as is as an additional identifier/selector on the IKEv2 level when negotiating CHILD_SAs and selecting configs. Labels are not installed in the kernel and received labels have to match exactly.
selinux - Only allowed if SELinux is usable on the system. The configured label is expected to be a generic context for which flows whose context match it via association:polmatch will trigger an acquire if no SA exists yet for the flow's specific context.
Type: String enum of system, simple, selinux.
Default: system

3.8.29.34 tfc_padding

Property: definitions :: vpn :: children_base :: tfc_padding

Description: Pads ESP packets with additional data to have a consistent ESP packet size for improved Traffic Flow Confidentiality. The padding defines the minimum size of all ESP packets sent. The default value of 0 disables TFC padding, the special value mtu adds TFC padding to create a packet size equal to the Path MTU.
Type: Enum of mtu.
Or
Type: Integer with a minimum of 0.
Default: 0

3.8.29.35 replay_window

Property: definitions :: vpn :: children_base :: replay_window
Description: IPsec replay window to configure for this CHILD_SA. Larger values than the default of 32 are supported using the Netlink backend only, a value of 0 disables IPsec replay protection.
Type: Integer with a minimum of 0 and a maximum of 32.
Default: 32

3.8.29.36 hw_offload

Property: definitions :: vpn :: children_base :: hw_offload
Description: Enable hardware offload for this CHILD_SA, if supported by the IPsec implementation. The value true enforces offloading and the installation will fail if it's not supported by either kernel or device. The value auto enables offloading if it's supported but the installation does not fail otherwise.
Type: Boolean true or false.
Or
Type: Enum of auto.
Default: False

3.8.29.37 copy_df

Property: definitions :: vpn :: children_base :: copy_df
Description: Whether to copy the DF bit to the outer IPv4 header in tunnel mode, effectively disabling Path MTU discovery. Controlling this behavior is not supported by all kernel interfaces.
Type: Boolean true or false.
Default: True

3.8.29.38 copy_ecn

Property: definitions :: vpn :: children_base :: copy_ecn
Description: Whether to copy the ECN (Explicity Congestion Notification) header field to/from the outer IP header in tunnel mode. Controlling this behavior is not supported by all kernel interfaces.
Type: Boolean true or false.
Default: True

3.8.29.39 copy_dscp

Property: definitions :: vpn :: children_base :: copy_dscp
Description: Whether to copy the DSCP (Differentiated Services Codepoint) header field to/from the outer IP header in tunnel mode.
out - Only copy the field from the inner to the outer header
in - Only copy the field from the outer to the inner header when decapsulating
true - Copy the field in both directions
false - Disable copying the field altogether
Controlling this behavior is not supported by all kernel interfaces.
Type: Boolean true or false.
Or
Type: Enum of in, out.
Default: True

3.8.29.40 start_action

Property: definitions :: vpn :: children_base :: start_action
Description: Action to perform after loading the configuration.
none (default) - Loads the connection only, which can then be manually initiated or used as a responder configuration
trap - Installs a trap policy which triggers the tunnel as soon as matching traffic has been detected
start - Initiates the connection actively
trap|start - Immediately initiate a connection for which trap policies have been installed.
Inverse actions are performed when unloading or replacing a CHILD_SA configuration with a start_action other than none.
Type: String enum of none, trap, start, trap|start.
Default: none

3.8.29.41 close_action

Property: definitions :: vpn :: children_base :: close_action
Description: Action to perform after a CHILD_SA gets closed by the peer.
none - Take no action
trap - Install a trap policy for the CHILD_SA
start - Immediately try to re-create the CHILD_SA
close_action must be none if the peer uses reauthentication or uniqueids checking, as these events might trigger the defined action when not desired.
Type: String enum of none, trap, start.
Default: none

3.8.30 connection_base

Property: definitions :: vpn :: connection_base
Description: A specific VPN connection
Type: JSON Object
Default: None

3.8.30.1 connection_base :: <pattern>

Property: definitions :: vpn :: connection_base :: ^(?!local_(addrs|port))local[a-zA-Z0-9_-]{0,20}$
Description: Section for a single local authentication round, defining the rules for how authentication is performed for the local peers.
Type: JSON Object
And
Type: Refer to - definitions->vpn->AuthRound
round: True
auth: True
id: True
eap_id: True
certs: True
pubkeys: True
Default: None

3.8.30.1.1 aaa_id

Property: definitions :: vpn :: connection_base :: ^(?!local_(addrs|port))local[a-zA-Z0-9_-]{0,20}$ :: aaa_id
Description: Server side EAP-Identity to expect in the EAP method.
Type: String.
Default: None

3.8.30.1.2 xauth_id

Property: definitions :: vpn :: connection_base :: ^(?!local_(addrs|port))local[a-zA-Z0-9_-]{0,20}$ :: xauth_id
Description: Client XAuth username used in the XAuth exchange.
Type: String.
^(?!certs)cert[a-zA-Z0-9_-]{0,20}$: True
Default: None

3.8.30.2 connection_base :: <pattern>

Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$
Description: Section for a single remote authentication round defining the constraints for how peers must authenticate to use this connection.
Type: JSON Object
And
Type: Refer to - definitions->vpn->AuthRound
round: True
auth: True
id: True
eap_id: True
certs: True
pubkeys: True

Default: None

3.8.30.2.1 groups
Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: groups
Description: Authorization group memberships to require; the peer must prove membership to at least one of the specified groups.
Type: Array of unique items.
Item type: String.
Default: None

3.8.30.2.2 cert_policy
Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: cert_policy
Description: List of certificate policy OIDs the peer's certificate must have. OIDs are specified using the numerical dotted representation.
Type: Array of unique items.
Item type: String pattern of ^([0-9]+\.)+[0-9]+$.
Default: None

3.8.30.2.3 cacerts
Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: cacerts
Description: List of CA certificates to accept for authentication.
Type: Array of unique items.
Type: Refer to - definitions->pki->file
Default: None

3.8.30.2.4 ca_id
Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: ca_id
Description: Identity in CA certificate to accept for authentication. The specified identity must be contained in one (intermediate) CA of the remote peer trustchain, either as the subject DN or as a subjectAltName. This has the same effect as specifying Cacerts to force clients under a CA to specific connections.
Type: String.
Default: None

3.8.30.2.5 revocation
Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: revocation
Description: Certificate revocation policy for CRL or OCSP revocation.
strict - Fails if no revocation information is available, i.e. the certificate is not known to be unrevoked

ifuri - Fails only if a CRL/OCSP URI is available but certificate revocation checking fails, i.e. there should be revocation information available but it could not be obtained
relaxed - Fails only if a certificate is revoked, i.e. it is explicitly known that it is bad
Type: String enum of strict, ifuri, relaxed.
Default: relaxed
^(?!certs)cert[a-zA-Z0-9_-]{0,20}$: True
Default: None

3.8.30.2.6 ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: <pattern>

Property: definitions :: vpn :: connection_base :: ^(?!remote_(addrs|port))remote[a-zA-Z0-9_-]{0,20}$ :: ^(?!cacerts)cacert[a-zA-Z0-9_-]{0,20}$
Type: Refer to - definitions->vpn->SingleCert
Default: None

3.8.30.3 References

Property: definitions :: vpn :: connection_base :: References
Description: List of other connections sections, or default connection sections, that will be inherited into this connection
Type: Array with a minimum number of 1 item(s) that must be unique.
Item type: String pattern of ^(connections\.)?[a-zA-Z0-9_-\.]+$.
Default: None

3.8.30.4 version

Property: definitions :: vpn :: connection_base :: version
Description: IKE major version to use for connection. 1 uses IKEv1 (aka ISAKMP), 2 uses IKEv2. A connection using the default of 0 accepts both IKEv1 and IKEv2 as a responder and initiates the connection actively with IKEv2.
Type: Enum of 0, 1, 2.
Default: 0

3.8.30.5 local_addrs

Property: definitions :: vpn :: connection_base :: local_addrs
Description: Local address(es) to use for IKE communication. Accepts single IPv4/IPv6 addresses, DNS names, CIDR subnets (10.1.0.0/16), or IP address ranges (10.1.0.0-10.2.255.255). While one can freely combine these items, to initiate a connection at least one non-range/subnet is required. As a responder, the local destination address must match at least one of the specified addresses, subnets, or ranges.
Type: Array of unique items.
Or
Type: Refer to - definitions->types->IPAddressMaskOpt
Or
Type: Refer to - definitions->types->IPAddressRange
Type: Refer to - definitions->types->FQDN
Or

Item type: Enum of %any.
Default: ['%any']

3.8.30.6 remote_addrs

Property: definitions :: vpn :: connection_base :: remote_addrs
Description: Remote address(es) to use for IKE communication. Accepts single IPv4/IPv6 addresses, DNS names, CIDR subnets (10.1.0.0/16), or IP address ranges (10.1.0.0-10.2.255.255). While one can freely combine these items, to initiate a connection at least one non-range/subnet is required. As a responder, the initiator source address must match at least one of the specified addresses, subnets, or ranges.
Type: Array of unique items.
Or
Type: Refer to - definitions->types->IPAddressMaskOpt
Or
Type: Refer to - definitions->types->IPAddressRange
Type: Refer to - definitions->types->FQDN
Or
Item type: Enum of %any.
Default: ['%any']

3.8.30.7 local_port

Property: definitions :: vpn :: connection_base :: local_port
Description: Local UDP port for IKE communication. If the default of port 500 is used, automatic IKE port floating to port 4500 is used to work around NAT issues Using a non-default local IKE port requires use of the socket-dynamic plugin.
Type: Refer to - definitions->types->Port
Default: 500

3.8.30.8 remote_port

Property: definitions :: vpn :: connection_base :: remote_port
Description: Remote UDP port for IKE communication. If the default of port 500 is used, automatic IKE port floating to port 4500 is used to work around NAT issues
Type: Refer to - definitions->types->Port
Default: 500
proposals: True
Default: None

3.8.30.9 vips

Property: definitions :: vpn :: connection_base :: vips
Description: List of virtual IPs to request in IKEv2 configuration payloads or IKEv1 ModeConfig. The wildcard addresses 0.0.0.0 and :: request an arbitrary address. If a specific IP address is configured, it will be requested from the responder, which is free to respond with a different address.
Type: Refer to - definitions->types->IPAddressArr

Default: None

3.8.30.10 pull

Property: definitions :: vpn :: connection_base :: pull
Description: If true, ModeConfig works in "pull" mode where the initiator actively requests a virtual IP. If false, "push" mode (IKEv1 only) is used where the responder pushes down a virtual IP to the initiating peer.
Type: Boolean true or false.
Default: True

3.8.30.11 dscp

Property: definitions :: vpn :: connection_base :: dscp
Description: The DSCP value to set on outgoing IKE packets for this connection.
Type: Refer to - definitions->types->DSCP
Default: 0

3.8.30.12 encap

Property: definitions :: vpn :: connection_base :: encap
Description: Enforce UDP encapsulation of ESP packets by manipulating the NAT detection payloads. This is usually not required but can help to work around connectivity issues with too-restrictive intermediary firewalls that block ESP packets.
Type: Boolean true or false.
Default: False

3.8.30.13 mobike

Property: definitions :: vpn :: connection_base :: mobike
Description: Enable/disable MOBIKE on IKEv2 connections. Allows mobility of clients and multi-homing on servers by migrating active IPsec tunnels (protocol defined in RFC 4555).
Type: Boolean true or false.
Default: True

3.8.30.14 dpd_delay

Property: definitions :: vpn :: connection_base :: dpd_delay
Description: The time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. In IKEv2, a value of 0s sends no additional INFORMATIONAL messages and uses only standard messages (such as those to rekey) to detect dead peers.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: 30s

3.8.30.15 dpd_timeout

Property: definitions :: vpn :: connection_base :: dpd_timeout

Description: The timeout interval after which all connections to a peer are deleted in case of inactivity. This only applies to IKEv1; in IKEv2 the default strongswan global retransmission timeout configuration applies, as every exchange is used to detect dead peers.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: 30s

3.8.30.16 fragmentation

Property: definitions :: vpn :: connection_base :: fragmentation
Description: Use IKE fragmentation (proprietary IKEv1 extension or RFC 7383 IKEv2 fragmentation). Acceptable values are yes, accept, force, and no.
yes - Oversized IKE messages will be sent in fragments (if the peer supports it)
accept - Support for fragmentation is announced to the peer but the daemon does not send its own messages in fragments
force - The initial IKE message will already be fragmented if required (IKEv1 only)
no - Disable announcing support for fragmentation
Type: String enum of yes, accept, force, no.
Default: yes

3.8.30.17 childless

Property: definitions :: vpn :: connection_base :: childless
Description: Use childless IKA_SA initiation (RFC 6023) for IKEv2. Acceptable values are allow, force, and never.
allow - Responders will accept childless IKA_SAs while initiators continue to create regular IKE_SAs with the first CHILD_SA created during IKE_AUTH, unless the IKA_SA is initiated explicitly without any children
force - Only childless initiation is accepted and the first CHILD_SA is created with a separate CREATE_CHILD_SA exchange
never - Disable support for childless IKE_SAs as responder
Type: String enum of allow, force, never.
Default: allow

3.8.30.18 send_certreq

Property: definitions :: vpn :: connection_base :: send_certreq
Description: Send certificate request payloads to offer trusted root CA certificates to the peer.
Type: Boolean true or false.
Default: True

3.8.30.19 send_cert

Property: definitions :: vpn :: connection_base :: send_cert
Description: Send certificate payloads when using certificate authentication.
ifasked - Send certificate payloads only if certificate requests have been received
never - Disable sending of certificate payloads
always - Send certificate payloads whenever certificate-based authentication is used
Type: String enum of ifasked, never, always.

Default: ifasked

3.8.30.20 ppk_id

Property: definitions :: vpn :: connection_base :: ppk_id
Description: Identifier of the Postquantum Preshared Key (PPK, RFC 8784) to be used
Type: String pattern of ^[a-zA-Z0-9+=\/]+$.
Default: None

3.8.30.21 ppk_required

Property: definitions :: vpn :: connection_base :: ppk_required
Description: Whether a PPK is required for this connection.
Type: Boolean true or false.
Default: False

3.8.30.22 keyingtries

Property: definitions :: vpn :: connection_base :: keyingtries
Description: Number of retransmission sequences to perform during initial connect. A value of 0 initiates a new sequence until the connection establishes or fails with a permanent error.
Type: Refer to - definitions->types->UINT32
Default: 1

3.8.30.23 unique

Property: definitions :: vpn :: connection_base :: unique
Description: To avoid multiple connections from the same user, a uniqueness policy can be enforced.
never - Never enforce a uniqueness policy
no - Replace existing connections for the same identity if a new one has the INITIAL_CONTACT notification
keep - Reject new connection attempts if the same user already has an active connection
replace - Delete any existing connection if a new one for the same user is established
Type: String enum of never, no, keep, replace.
Default: no

3.8.30.24 reauth_time

Property: definitions :: vpn :: connection_base :: reauth_time
Description: Interval after which to schedule IKE reauthentication. A value of 0 disables reauthentication.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: 0s

3.8.30.25 rekey_time

Property: definitions :: vpn :: connection_base :: rekey_time
Description: Interval after which to refresh key material using a Diffie-Hellman key exchange (IKEv2 only; IKEv1 performs a reauth instead). If a reauth_time is configured, rekey_time

defaults to zero, disabling rekeying. rekey_time can still be explicitly set to enforce both rekeying and reauthentication.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: 4h

3.8.30.26 over_time

Property: definitions :: vpn :: connection_base :: over_time
Description: Hard IKE_SA lifetime limit if rekey/reauth does not complete. If the IKE_SA fails to rekey or reauthenticate within the specified time, it is closed. Default is 10% of reauth_time or rekey_time, whichever is larger.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: None

3.8.30.27 rand_time

Property: definitions :: vpn :: connection_base :: rand_time
Description: Time range from which to choose a random value to subtract from rekey/reauth times. The default is equal to the configured over_time.
Type: String pattern of ^(0|[1-9][0-9]{0,4})(d|h|m|s)$.
Default: None

3.8.30.28 pools

Property: definitions :: vpn :: connection_base :: pools
Description: List of named IP pools to allocate virtual IP addresses and other configuration attributes from. Each name references a pool from the Pools section or an external pool. Only if pools are provided by the same backend does the order matter.
Type: Array of unique items.
Item type: String pattern of ^[a-zA-Z0-9_-]+$.
Default: None

3.8.30.29 if_id_in

Property: definitions :: vpn :: connection_base :: if_id_in
Description: XFRM interface ID set on in-bound policies/SA. Can be overridden by child configuration.
The special value %unique allocates a unique interface ID per IKE_SA, which is inherited by all its CHILD_SAs (unless overridden there).
The special value %unique-dir assigns a different unique interface ID for each direction (in/out).
Type: Refer to - definitions->vpn->if_id
Default: 0

3.8.30.30 if_id_out

Property: definitions :: vpn :: connection_base :: if_id_out
Description: XFRM interface ID set on out-bound policies/SA. Can be overridden by child configuration.

The special value %unique allocates a unique interface ID per IKE_SA, which is inherited by all its CHILD_SAs (unless overridden there).
The special value %unique-dir assigns a different unique interface ID for each direction (in/out).
Type: Refer to - definitions->vpn->if_id
Default: 0

3.8.30.31 mediation

Property: definitions :: vpn :: connection_base :: mediation
Description: Whether this connection is a mediation connection, i.e. whether this connection is used to mediate other connections using the IKEv2 Mediation Extension. Mediation connections create no CHILD_SA.
Type: Boolean true or false.
Default: False

3.8.30.32 mediated_by

Property: definitions :: vpn :: connection_base :: mediated_by
Description: The name of the connection to mediate this connection through, if given. The mediation connection must have mediation enabled.
Type: String.
Type: Refer to - definitions->types->AlphaNumeric
Default: None

3.8.30.33 mediation_peer

Property: definitions :: vpn :: connection_base :: mediation_peer
Description: Identity under which the peer is registered at the mediation server, i.e. the IKE identity the other end of this connection uses as its local identity on its connection to the mediation server. Only relevant on connections that set mediated_by. If not given, the remote IKE identity of the first authentication round of this connection will be used.
Type: String.
children: True
Default: None

3.8.31 connection_base_niap

Property: definitions :: vpn :: connection_base_niap
And
Type: Refer to - definitions->vpn->connection_base
Default: None

3.8.31.1 proposals

Property: definitions :: vpn :: connection_base_niap :: proposals
Description: List of sets of algorithms.
Non-AEAD algorithms: encryption algorithm, integrity algorithm, (optional) pseudo-random function, Diffie-Hellman key exchange group.

AEAD algorithms: combined algorithm (instead of encryption and integrity), pseudo-random function, Diffie-Hellman key exchange group.
With IKEv2 multiple algorithms of the same kind can be specified in a single proposal, from which one gets selected. For IKEv1 only one algorithm of each kind is allowed per proposal, additional algorithms are implicitly stripped.
Type: JSON Object
Default: None

3.8.31.2 list
Property: definitions :: vpn :: connection_base_niap :: proposals :: list
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->vpn->NIAPAEADProposal
Or
Type: Refer to - definitions->vpn->NIAPNonAEADProposal
Default: None

3.8.31.3 children
Property: definitions :: vpn :: connection_base_niap :: children
Description: CHILD_SA configuration subsections.
Type: JSON Object
Default: None

3.8.31.3.1 children :: <pattern>
Property: definitions :: vpn :: connection_base_niap :: children :: ^[a-zA-Z0-9_-]+$
Type: Refer to - definitions->vpn->children_base_niap
Default: None

3.8.32 children_base_niap
Property: definitions :: vpn :: children_base_niap
And
Type: Refer to - definitions->vpn->children_base
Default: None

3.8.32.1 esp_proposals
Property: definitions :: vpn :: children_base_niap :: esp_proposals
Description: Encapsulating Security Payload (ESP) proposals (sets of algorithms) to offer for the CHILD_SA.
Non-AEAD proposals: encryption algorithm, integrity algorithm, optional Diffie-Hellman group, optional Extended Sequence Number Mode (ESN) indicator.
Type: JSON Object
Required: ['list']
Default: None

3.8.32.1.1 list

Property: definitions :: vpn :: children_base_niap :: esp_proposals :: list
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->vpn->NIAPESPProposal
Default: None

3.8.32.2 ah_proposals
Property: definitions :: vpn :: children_base_niap :: ah_proposals
Description: Authentication Header (AH) proposals (sets of algorithms) to offer for the CHILD_SA. Order: integrity algorithm, optional Diffie-Hellman group.
Type: JSON Object
Required: ['list']
Default: None

3.8.32.2.1 list
Property: definitions :: vpn :: children_base_niap :: ah_proposals :: list
Type: Array of unique items and a minimum number of 1 item(s).
Type: Refer to - definitions->vpn->NIAPAHProposal
Default: None

3.9 radiocontroller
Property: definitions :: radiocontroller
Default: None

3.9.1 BaseLink
Property: definitions :: radiocontroller :: BaseLink
Required: ['Link', 'RadioType']
Default: None

3.9.1.1 Link
Property: definitions :: radiocontroller :: BaseLink :: Link
Description: The name of the link that the radio is attached to, this must match a named link in the ARES core configuration.
Type: Refer to - definitions->types->InterfaceName
Default: None

3.9.2 HALORXModes
Property: definitions :: radiocontroller :: HALORXModes
Type: String enum of bemode1, bemode2, bemode3, bemode4, bemode6, bemode104_2mbps, bemode104_4mbps, bemode104_10mbps, bemode104_20mbps, bemode104_44mbps, cubic2, cubic4, br10.71b, br21.42, br44.73.
Default: None

3.9.3 HALOLink
Property: definitions :: radiocontroller :: HALOLink
Required: ['Beams', 'Endpoints']
Default: None

3.9.3.1 RadioType
Property: definitions :: radiocontroller :: HALOLink :: RadioType
Description: The type of the radio to be controlled on this link.
Type: String enum of halo.
Default: None

3.9.3.2 Beams
Property: definitions :: radiocontroller :: HALOLink :: Beams
Description: An array of beam configurations of the HALO radio.
Type: Array with a minimum number of 1 item(s) and a maximum number of 12 item(s) that must be unique.
Item description: HALO Beam configuration
Item type: JSON Object
Required: ['Number', 'Channels']
Default: None

3.9.3.2.1 Number
Property: definitions :: radiocontroller :: HALOLink :: Beams :: Number
Item description: The HALO beam number, 0-11.
Item type: Integer with a minimum of 0 and a maximum of 11.
Default: None

3.9.3.2.2 Channels
Property: definitions :: radiocontroller :: HALOLink :: Beams :: Channels
Item description: An array of channel numbers that are supported by this beam.
Item type: Array with a minimum number of 1 item(s) and a maximum number of 42 item(s) that must be unique.
Item description: A supported channel number, 0-41 (0-21 = LO - LO+105MHz, 22-41 = LO-100MHz - LO-5MHz).
Item type: Integer with a minimum of 0 and a maximum of 41.
Default: None

3.9.3.3 Endpoints
Property: definitions :: radiocontroller :: HALOLink :: Endpoints
Description: An array of endpoint configurations for all possible endpoints in the HALO radio network.
Type: Array with a minimum number of 1 item(s) that must be unique.
Item description: HALO Endpoint configuration.
Item type: JSON Object

Required: ['ID', 'Mode', 'Channel']
Default: None

3.9.3.3.1 ID

Property: definitions :: radiocontroller :: HALOLink :: Endpoints :: ID
Item description: The ARES router ID of the endpoint.
Type: Refer to - definitions->types->UINT32
Or
Type: Refer to - definitions->types->DottedQuad
Default: None

3.9.3.3.2 Channel

Property: definitions :: radiocontroller :: HALOLink :: Endpoints :: Channel
Item description: The operating channel of the endpoint.
Item type: Integer with a minimum of 0 and a maximum of 41.
Default: None

3.9.3.3.3 Mode

Property: definitions :: radiocontroller :: HALOLink :: Endpoints :: Mode
Item description: The operating RX mode of the endpoint.
Type: Refer to - definitions->radiocontroller->HALORXModes
Default: None

3.9.3.4 StandardDeviationLimit

Property: definitions :: radiocontroller :: HALOLink :: StandardDeviationLimit
Description: The lowest the calculated standard deviation can be in a single BSS capture in order for signal detection to occur. If the STDEV is lower than this number, then it is assumed that there is just background noise in the capture and no signals to detect.
Type: Integer with a minimum of 30 and a maximum of 200.
Default: 50

3.9.3.5 StandardDeviationFactor

Property: definitions :: radiocontroller :: HALOLink :: StandardDeviationFactor
Description: The number of standard deviations a signal must be above the average in a BSS capture before it is considered a unique signal.
Type: Number.
Default: 3.5

3.10 visualizer

Property: definitions :: visualizer
Default: None

3.10.1 VisualizerInformation
Property: definitions :: visualizer :: VisualizerInformation
Type: String enum of gps, routes, firewall, metrics, flows, links, attacks, display.
Default: None

3.11 BitSources

Property: definitions :: BitSources
Default: None

3.11.1 OnTime
Property: definitions :: BitSources :: OnTime
Type: JSON Object
Required: ['Source']
Default: None

3.11.1.1 Source
Property: definitions :: BitSources :: OnTime :: Source
Description: The source for BIT information.
Type: String enum of ontime.
Default: None

3.11.1.2 Community
Property: definitions :: BitSources :: OnTime :: Community
Description: Community string for OnTime Networks switch SNMP.
Type: String with a minimum length of 0 and a maximum Length of 255 characters and a pattern of ^[!-~]{0,255}$.
Default: private

3.11.1.3 SNMPAddress
Property: definitions :: BitSources :: OnTime :: SNMPAddress
Description: The switch IP address where SNMP is running.
Type: Refer to - definitions->types->IPAddress
Default: 192.168.10.1

3.11.1.4 SNMPPort
Property: definitions :: BitSources :: OnTime :: SNMPPort
Description: The UDP port for SNMP.
Type: Refer to - definitions->types->Port
Default: SNMP-default

3.12 ZOOM

Property: definitions :: ZOOM
Default: None

3.12.1 SubnetMap

Property: definitions :: ZOOM :: SubnetMap
Type: Array of unique items and a maximum number of 2047 item(s).
Item description: A subnet mapping of ID->Subnet for ZOOM/TSCANR.
Item type: JSON Object
Required: ['ID', 'Subnet']
Default: None

3.12.1.1 ID

Property: definitions :: ZOOM :: SubnetMap :: ID
Item type: String pattern of ^(\((([1-9][0-9]{0,2}|1[0-9]{0,3}|20[0-4][0-7])-([1-9][0-9]{0,2}|1[0-9]{0,3}|20[0-4][0-7]))\)|([1-9][0-9]{0,2}|1[0-9]{0,3}|20[0-4][0-7]))$.
Default: None

3.12.1.2 Subnet

Property: definitions :: ZOOM :: SubnetMap :: Subnet
Item description: Supports ranged subnets.
Examples:
192.168.0.0/24 // A simple single subnet.
192.168.(1-100).0/24 // A ranged subnet including everything from 192.168.1.0/24 to 192.168.100.0/24.
10.(1-10).(100-200).0/24 // A ranged subnet with multiple octets.
Type: Refer to - definitions->types->DottedQuadRangeMaskReq
Default: None

3.13 dhcp

Property: definitions :: dhcp
Default: None

3.13.1 OptionData4

Property: definitions :: dhcp :: OptionData4
Description: Standard DHCPv4 options.
Type: JSON Object
Default: None

3.13.1.1 DomainName

Property: definitions :: dhcp :: OptionData4 :: DomainName
Description: Domain name of the local network.

Type: Refer to - definitions->types->FQDN
Default: None

3.13.1.2 DNS
Property: definitions :: dhcp :: OptionData4 :: DNS
Description: DNS servers to advertise to clients.
Type: Refer to - definitions->types->IPv4AddressArr
Default: None

3.13.1.3 Routers
Property: definitions :: dhcp :: OptionData4 :: Routers
Description: Router addresses to advertise to clients.
Type: Refer to - definitions->types->IPv4AddressArr
Default: None

3.13.1.4 BroadcastAddress
Property: definitions :: dhcp :: OptionData4 :: BroadcastAddress
Description: Broadcast address to advertise to clients.
Type: Refer to - definitions->types->IPv4Address
Default: None

3.13.1.5 OtherOptions
Property: definitions :: dhcp :: OptionData4 :: OtherOptions
Description: A catch-all for any other standard DHCPv4 options.
Type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Required: ['Name']
Default: None

3.13.1.5.1 Name
Property: definitions :: dhcp :: OptionData4 :: OtherOptions :: Name
Item description: The name of the option to configure.
Item type: String pattern of ^[a-zA-Z0-9-]+$.
Default: None

3.13.1.5.2 Data
Property: definitions :: dhcp :: OptionData4 :: OtherOptions :: Data
Item description: The configuration to be applied.
Item type: String.
Default: None

3.13.2 OptionData6
Property: definitions :: dhcp :: OptionData6

Description: Standard DHCPv6 options.
Type: JSON Object
Default: None

3.13.2.1 DNS
Property: definitions :: dhcp :: OptionData6 :: DNS
Description: DNS servers to advertise to clients.
Type: Refer to - definitions->types->IPv6AddressArr
Default: None

3.13.2.2 OtherOptions
Property: definitions :: dhcp :: OptionData6 :: OtherOptions
Description: A catch-all for any other standard DHCPv6 options.
Type: Array of unique items and a minimum number of 1 item(s).
Item type: JSON Object
Required: ['Name']
Default: None

3.13.2.2.1 Name
Property: definitions :: dhcp :: OptionData6 :: OtherOptions :: Name
Item description: The name of the option to configure.
Item type: String pattern of ^[a-zA-Z0-9-]+$.
Default: None

3.13.2.2.2 Data
Property: definitions :: dhcp :: OptionData6 :: OtherOptions :: Data
Item description: The configuration to be applied.
Item type: String.
Default: None

3.14 Sysctl
Property: definitions :: Sysctl
Default: None

3.14.1 Net
Property: definitions :: Sysctl :: Net
Default: None

3.14.1.1 IPv4
Property: definitions :: Sysctl :: Net :: IPv4
Default: None

3.14.1.1.1 Conf
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf
Description: IPv4 parameters.
Type: JSON Object
Default: None

3.14.1.1.1.1AcceptLocal
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: AcceptLocal
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.2AcceptRedirects
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: AcceptRedirects
Description: Accept ICMP redirect messages.
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.3AcceptSourceRoute
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: AcceptSourceRoute
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.4ArpAccept
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ArpAccept
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.5ArpAnnounce
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ArpAnnounce
Description: Define different restriction levels for announcing the local source IP address from IP packets in ARP requests sent on interface: 0 - use any local address, configured on any interface. 1 - Try to avoid local addresses that are not in the target's subnet for this interface. 2 - Always use the best local address for this target.
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 2

3.14.1.1.1.6ArpFilter
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ArpFilter
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.7ArpIgnore
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ArpIgnore
Description: Define different modes for sending replies in response to received ARP requests that resolve local target IP addresses: 0 - reply for any local target IP address, configured on any interface. 1 - reply only if the target IP address is local address configured on the incoming

interface. 2 - reply only if the target IP address is local address configured on the incoming interface and both with the sender's IP address are part from same subnet on this interface. 3 - do not reply for local addresses configured with scope host, only resolutions for global and link addresses are replied. 4-7 - reserved. 8 - do not reply for all local addresses
Type: Integer with a minimum of 0 and a maximum of 8.
Default: 1

3.14.1.1.1.8ArpNotify
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ArpNotify
Description: Define mode for notification of address and device changes: 0 - do nothing. 1 - generate gratuitous ARP requests when device is brought up or hardware address changes.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.9BootpRelay
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: BootpRelay
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.10 DisablePolicy
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: DisablePolicy
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.11 DisableXfrm
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: DisableXfrm
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.12 DropGratuitousArp
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: DropGratuitousArp
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.13 DropUnicastInL2Multicast
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: DropUnicastInL2Multicast
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.14 ForceIgmpVersion
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ForceIgmpVersion
Type: Integer with a minimum of 0 and a maximum of 3.
Default: 0

3.14.1.1.1.15 Forwarding
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: Forwarding

Description: Enable IP forwarding on this interface. This controls whether packets received on this interface can be forwarded.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.16 Igmpv2UnsolicitedReportInterval
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: Igmpv2UnsolicitedReportInterval
Type: Integer.
Default: 10000

3.14.1.1.1.17 Igmpv3UnsolicitedReportInterval
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: Igmpv3UnsolicitedReportInterval
Type: Integer.
Default: 1000

3.14.1.1.1.18 IgnoreRoutesWithLinkdown
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: IgnoreRoutesWithLinkdown
Description: Ignore routes whose link is down when performing an FIB lookup.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.19 LogMartians
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: LogMartians
Description: Log packets with impossible addresses to kernel log.
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.20 McForwarding
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: McForwarding
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.21 *MediumId*
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: MediumId
Type: Integer.
Default: 0

3.14.1.1.1.22 PromoteSecondaries
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: PromoteSecondaries
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.23 ProxyArp
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ProxyArp
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.24 ProxyArpPvlan
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: ProxyArpPvlan
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.25 RouteLocalnet
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: RouteLocalnet
Type: Refer to - definitions->types->BooleanInt
Default: 0

RpFilter
3.14.1.1.1.26 Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: RpFilter
Description: 0 - No source validation. 1 - Strict mode as defined in RFC3704 Strict Reverse Path. Each incoming packet is tested against the FIB and if the interface is not the best reverse path the packet check will fail. By default failed packets are discarded. 2 - Loose mode as defined in RFC3704 Loose Reverse Path. Each incoming packet's source address is also tested against the FIB and if the source address is not reachable via any interface the packet check will fail.
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

3.14.1.1.1.27 SecureRedirects
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: SecureRedirects
Description: Accept ICMP redirect messages only to gateways listed in the interface's current gateway list. Overridden by SharedMedia.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.28 SendRedirects
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: SendRedirects
Description: Send redirects, if router.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.29 SharedMedia
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: SharedMedia
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.1.1.30 SrcValidMark
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: SrcValidMark
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.1.1.31 Tag
Property: definitions :: Sysctl :: Net :: IPv4 :: Conf :: Tag

Type: Integer.
Default: 0

3.14.1.2 IPv6
Property: definitions :: Sysctl :: Net :: IPv6
Default: None

3.14.1.2.1 Conf
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf
Description: IPv6 parameters.
Type: JSON Object
Default: None

3.14.1.2.1.1AcceptDad
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptDad
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 1

3.14.1.2.1.2AcceptRa
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRa
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 1

3.14.1.2.1.3AcceptRaDefrtr
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaDefrtr
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.4AcceptRaFromLocal
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaFromLocal
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.5AcceptRaMinHopLimit
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaMinHopLimit
Type: Integer.
Default: 1

3.14.1.2.1.6AcceptRaMtu
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaMtu
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.7AcceptRaPinfo
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaPinfo

Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.8AcceptRaRtInfoMaxPlen
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaRtInfoMaxPlen
Type: Integer.
Default: 0

3.14.1.2.1.9AcceptRaRtrPref
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRaRtrPref
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.10 AcceptRedirects
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptRedirects
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.11 AcceptSourceRoute
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: AcceptSourceRoute
Description: Accept packets with SRR option.
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.12 Autoconf
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: Autoconf
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.13 DadTransmits
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: DadTransmits
Type: Integer.
Default: 1

3.14.1.2.1.14 DisableIpv6
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: DisableIpv6
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.15 DropUnicastInL2Multicast
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: DropUnicastInL2Multicast
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.16 DropUnsolicitedNa
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: DropUnsolicitedNa

Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.17 ForceMldVersion
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: ForceMldVersion
Type: Integer with a minimum of 0 and a maximum of 2.
Default: 0

3.14.1.2.1.18 ForceTllao
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: ForceTllao
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.19 Forwarding
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: Forwarding
Description: Global: Enable IPv6 forwarding between all interfaces. Interface: Enable IPv6 forwarding on this interface.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.20 HopLimit
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: HopLimit
Type: Integer.
Default: 64

3.14.1.2.1.21 IgnoreRoutesWithLinkdown
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: IgnoreRoutesWithLinkdown
Description: Ignore routes whose link is down when performing an FIB lookup.
Type: Refer to - definitions->types->BooleanInt
Default: 1

3.14.1.2.1.22 KeepAddrOnDown
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: KeepAddrOnDown
Description: Keep all IPv6 addresses on an interface down event. If set static global addresses with no expiration time are not flushed. >0 - enabled. 0 - system default. <0 - disabled.
Type: Integer.
Default: 1

3.14.1.2.1.23 MaxAddresses
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: MaxAddresses
Type: Integer.
Default: 16

MaxDesyncFactor
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: MaxDesyncFactor
Type: Integer.

Default: 600

3.14.1.2.1.24 McForwarding
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: McForwarding
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.25 Mldv1UnsolicitedReportInterval
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: Mldv1UnsolicitedReportInterval
Type: Integer.
Default: 10000

3.14.1.2.1.26 Mldv2UnsolicitedReportInterval
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: Mldv2UnsolicitedReportInterval
Type: Integer.
Default: 1000

3.14.1.2.1.27 Mtu
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: Mtu
Type: Integer.
Default: 1280

3.14.1.2.1.28 NdiscNotify
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: NdiscNotify
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.29 OptimisticDad
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: OptimisticDad
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.30 ProxyNdp
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: ProxyNdp
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.31 RegenMaxEntry
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: RegenMaxEntry
Type: Integer.
Default: 3

3.14.1.2.1.32 RouterProbeInterval
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: RouterProbeInterval
Type: Integer.
Default: 60

3.14.1.2.1.33 RouterSolicitationDelay
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: RouterSolicitationDelay
Type: Integer.
Default: 1

3.14.1.2.1.34 RouterSolicitationInterval
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: RouterSolicitationInterval
Type: Integer.
Default: 4

3.14.1.2.1.35 RouterSolicitationMaxInterval
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: RouterSolicitationMaxInterval
Type: Integer.
Default: 3600

3.14.1.2.1.36 RouterSolicitations
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: RouterSolicitations
Type: Integer.
Default: -1

3.14.1.2.1.37 SuppressFragNdisc
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: SuppressFragNdisc
Type: Integer.
Default: 1

3.14.1.2.1.38 TempPreferedLft
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: TempPreferedLft
Type: Integer.
Default: 86400

3.14.1.2.1.39 TempValidLft
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: TempValidLft
Type: Integer.
Default: 604800

3.14.1.2.1.40 UseOifAddrsOnly
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: UseOifAddrsOnly
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.41 UseOptimistic
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: UseOptimistic
Type: Refer to - definitions->types->BooleanInt
Default: 0

3.14.1.2.1.42 UseTempaddr
Property: definitions :: Sysctl :: Net :: IPv6 :: Conf :: UseTempaddr
Type: Integer.
Default: 0

3.14.1.3 Neigh
Property: definitions :: Sysctl :: Net :: Neigh
Type: JSON Object
Default: None

3.14.1.3.1 AnycastDelay
Property: definitions :: Sysctl :: Net :: Neigh :: AnycastDelay
Type: Integer.
Default: 100

3.14.1.3.2 AppSolicit
Property: definitions :: Sysctl :: Net :: Neigh :: AppSolicit
Type: Integer.
Default: 0

3.14.1.3.3 BaseReachableTimeMs
Property: definitions :: Sysctl :: Net :: Neigh :: BaseReachableTimeMs
Description: Once a neighbor has been found, the entry is considered to be valid for at least a random value between base_reachable_time_ms/2 and 3*base_reachable_time_ms/2. An entry's validity will be extended if it receives positive feedback from higher level protocols.
Type: Integer.
Default: 14400000

3.14.1.3.4 DelayFirstProbeTime
Property: definitions :: Sysctl :: Net :: Neigh :: DelayFirstProbeTime
Type: Integer.
Default: 5

GcInterval
Property: definitions :: Sysctl :: Net :: Neigh :: GcInterval
Type: Integer.
Default: 30

3.14.1.3.5 GcStaleTime
Property: definitions :: Sysctl :: Net :: Neigh :: GcStaleTime
Type: Integer.
Default: 60

3.14.1.3.6 GcThresh1
Property: definitions :: Sysctl :: Net :: Neigh :: GcThresh1
Type: Integer.
Default: 128

3.14.1.3.7 GcThresh2
Property: definitions :: Sysctl :: Net :: Neigh :: GcThresh2
Description: Threshold when garbage collector becomes more aggressive about purging entries. Entries older than 5 seconds will be cleared when over this number.
Type: Integer.
Default: 3584

3.14.1.3.8 GcThresh3
Property: definitions :: Sysctl :: Net :: Neigh :: GcThresh3
Description: Maximum number of non-PERMANENT neighbor entries allowed. Increase this when using large numbers of interfaces and when communicating with large numbers of directly-connected peers.
Type: Integer.
Default: 4096

3.14.1.3.9 Locktime
Property: definitions :: Sysctl :: Net :: Neigh :: Locktime
Type: Integer.
Default: 0

3.14.1.3.10 McastResolicit
Property: definitions :: Sysctl :: Net :: Neigh :: McastResolicit
Type: Integer.
Default: 0

3.14.1.3.11 McastSolicit
Property: definitions :: Sysctl :: Net :: Neigh :: McastSolicit
Description: The maximum number of multicast probes in INCOMPLETE state, when the associated hardware address is unknown.
Type: Integer with a minimum of 1.
Default: 10

3.14.1.3.12 ProxyDelay
Property: definitions :: Sysctl :: Net :: Neigh :: ProxyDelay
Type: Integer.
Default: 80

3.14.1.3.13 ProxyQlen

Property: definitions :: Sysctl :: Net :: Neigh :: ProxyQlen
Type: Integer.
Default: 64

3.14.1.3.14 RetransTimeMs
Property: definitions :: Sysctl :: Net :: Neigh :: RetransTimeMs
Type: Integer.
Default: 1000

3.14.1.3.15 UcastSolicit
Property: definitions :: Sysctl :: Net :: Neigh :: UcastSolicit
Type: Integer.
Default: 3

3.14.1.3.16 UnresQlen
Property: definitions :: Sysctl :: Net :: Neigh :: UnresQlen
Type: Integer.
Default: 31

3.14.1.3.17 UnresQlenBytes
Property: definitions :: Sysctl :: Net :: Neigh :: UnresQlenBytes
Type: Integer.
Default: 65536

3.15 accounts

Property: definitions :: accounts
Default: None

3.15.1 AccountObject
Property: definitions :: accounts :: AccountObject
Description: User account information.
Type: JSON Object
Required: ['Name', 'Password']
Default: None

3.15.1.1 Name
Property: definitions :: accounts :: AccountObject :: Name
Description: The name of the user account.
Type: String pattern of ^(?!^(admin|administrator|root|sudo)$)([a-z_]([a-z0-9_-]{0,31}|[a-z0-9_-]{0,30}\$))$.
Default: None

3.15.1.2 Group
Property: definitions :: accounts :: AccountObject :: Group
Description: Group to which the account should belong.
Type: Enum of transport, users, config, security.
Default: users

3.15.1.3 Password
Property: definitions :: accounts :: AccountObject :: Password
Description: The password for the user account.
Type: Refer to - definitions->pki->password_or_pass
Default: None

3.15.1.4 SSHAuthorizedKeys
Property: definitions :: accounts :: AccountObject :: SSHAuthorizedKeys
Description: SSH public keys that can be used to SSH to the user account
Type: Array with a minimum number of 1 item(s) that must be unique.
Type: Refer to - definitions->pki->ssh_pubkey_or_file
Default: None

3.15.1.5 SSHKeyPairs
Property: definitions :: accounts :: AccountObject :: SSHKeyPairs
Type: Array with a minimum number of 1 item(s) that must be unique.
Item description: SSH key pair that belongs to the user account
Type: Refer to - definitions->pki->ssh_keypair
Description: Defines the parameters of an ARES router.
Type: JSON Object
Required: ['RouterId']
Default: None