



Nokia Service Router Linux

DATA MODEL REFERENCE Release R20.6

3HE 16123 AAAA TQZZA

Edition: 1

July 2020

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2020 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.

Table of Contents

1	Introduction	4
2	acl	8
3	bfd	410
4	interface	437
5	network-instance	550
6	platform	860
7	qos	942
8	routing-policy	949
9	system	967
10	tools acl	1109
11	tools bfd	1120
12	tools interface	1123
13	tools network-instance	1132
14	tools platform	1144
15	tools system	1156

1 Introduction

This document describes the configuration and state data models available for the Nokia Service Router Linux (SR Linux).



Note: This guide generically covers the current release and may contain some content that will be released in later maintenance loads. Refer to the *SR Linux Release Notes*, for information about features supported in each load.

For additional information about accessing and using the interfaces that support these data models, refer to the *SR Linux Interface Configuration Guide*.

1.1 Tree hierarchy

The tree hierarchy consists of branches that show the fields and parameters that are available. [Figure 1](#) shows a tree hierarchy example.

Figure 1 Tree hierarchy example

```
bfd
- network-instance string
- peer number
  - active-receive-interval
  - active-transmit-interval
  - async
  - last-packet-received
  - last-packet-transmitted
  - received-errored-packets
  - received-packets
  - transmitted-packets
  - up-transitions
  - failure-transitions
  - last-failure-time
  - local-address
  - local-diagnostic-code
  - oper-state
  - remote-address
  - remote-control-plane-independent
  - remote-diagnostic-code
  - remote-discriminator
  - remote-minimum-receive-interval
  - remote-multiplier
  - remote-session-state
  - session-state
  - subscribed-protocols
+ peers number
+ clear
+ statistics
```

Each chapter of this guide describes a branch in the tree with field names linked to their corresponding descriptions. These descriptions indicate the required syntax for each field. See [Field descriptions](#) for more information.

Italic names after a field indicate the parameter type. Parameter types include (but are not limited to):

- Boolean (true and false values)
- keyword (enumerated values)
- string
- number
- IPv4 prefix
- IPv6 prefix
- IPv4 address
- IPv6 address
- MAC address

For more information about the input values, click the field or parameter name in the tree. The link will take you to the description where these values are defined.

A parameter type may also be a combination of different base types. These parameters are displayed in the tree with the individual parameter types enclosed in round brackets and separated by a pipe. For example: *(keyword | number)*

1.2 Transaction and report types

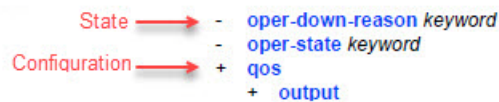
The following transaction and report types are used with the SR Linux:

- configuration transactions
- state transactions
- show reports

Configuration transactions allow you to modify a configuration while state transactions allow you to view the configuration and operational state.

In the tree hierarchy, configuration transactions are denoted with a plus sign (+). State transactions are denoted with a minus sign (-). See [Figure 2](#).

Figure 2 Configuration/state in tree hierarchy



Each field description has a field called “Configurable”. The field is set to either:

- true (for configuration transactions)
- false (for state transactions)

Show reports are Python plug-ins used to create custom output. A set of pre-defined show reports are provided and described in the *SR Linux Interface Configuration Guide*. These pre-defined reports can be used as examples for how to create additional custom reports.

1.3 Hardware platform designation

Transactions are valid on all platforms except where noted. For example, if a command is only valid on a specific platform, it will have a note like the following:



Note: This command is available on the following platforms:

- 7250 IXR-10
- 7250 IXR-6

1.4 Field descriptions

Syntax for each field is displayed in bold, followed by supported parameters and their type. In the example that follows, the **bfd network-instance** field shows that the parameter type is a string:

```
— bfd
   — network-instance string
```

[Table 1](#) describes valid fields for commands. Not all fields are applicable for all commands.

Table 1 Field descriptions

Field	Description
Context	Configuration path to the command
Tree	Defines the commands location in the tree hierarchy
Description	Describes the command
Configurable	Indicates if the command can be configured (true) or if it is a view-only state command (false)
String Length	For a string, indicates a range (number of characters allowed)
Range	For a number, indicates the range of allowed values
Default	Default value
Units	Base unit type
Options	Enumerated values allowed
Reference	Reference to an instance in the configuration needed before the configuration is considered valid
Max Element	For lists and leaf-lists, the maximum number of elements

1.4.1 References

A description of each parameter is also available from the online CLI help function. See the *SR Linux Interface Configuration Guide* for information on using the CLI help.

2 acl

acl

- + **capture-filter**
- + **ipv4-filter**
 - + **entry sequence-id** *number*
 - + **action**
 - + **accept**
 - + **copy**
 - + **description** *string*
 - + **match**
 - + **destination-address** *string*
 - + **destination-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **first-fragment** *boolean*
 - + **fragment** *boolean*
 - + **icmp**
 - + **code** *number*
 - + **type** (*number | keyword*)
 - + **protocol** (*number | keyword*)
 - + **source-address** *string*
 - + **source-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **tcp-flags** *string*
 - **tcam-entries** *number*
- + **ipv6-filter**
 - + **entry sequence-id** *number*
 - + **action**
 - + **accept**
 - + **copy**
 - + **description** *string*
 - + **match**
 - + **destination-address** *string*
 - + **destination-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **icmp6**
 - + **code** *number*
 - + **type** (*number | keyword*)
 - + **next-header** (*number | keyword*)
 - + **source-address** *string*

- + **source-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
- **tcam-entries** *number*
- + **cpm-filter**
 - + **ipv4-filter**
 - + **entry sequence-id** *number*
 - + **action**
 - + **accept**
 - + **log** *boolean*
 - + **rate-limit**
 - + **distributed-policer** *reference*
 - + **system-cpu-policer** *reference*
 - + **drop**
 - + **log** *boolean*
 - + **description** *string*
 - + **match**
 - + **destination-address** *string*
 - + **destination-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **first-fragment** *boolean*
 - + **fragment** *boolean*
 - + **icmp**
 - + **code** *number*
 - + **type** (*number | keyword*)
 - + **protocol** (*number | keyword*)
 - + **source-address** *string*
 - + **source-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **tcp-flags** *string*
 - **statistics**
 - **distributed-policer**
 - **conforming-octets** *number*
 - **conforming-packets** *number*
 - **exceeding-octets** *number*
 - **exceeding-packets** *number*
 - **last-clear** *string*
 - **last-match** *string*
 - **matched-packets** *number*
 - **system-cpu-policer**
 - **conforming-octets** *number*
 - **conforming-packets** *number*

- **exceeding-octets** *number*
- **exceeding-packets** *number*
- **tcam-entries** *number*
- **last-clear** *string*
- + **statistics-per-entry** *boolean*
- + **ipv6-filter**
 - + **entry sequence-id** *number*
 - + **action**
 - + **accept**
 - + **log** *boolean*
 - + **rate-limit**
 - + **distributed-policer** *reference*
 - + **system-cpu-policer** *reference*
 - + **drop**
 - + **log** *boolean*
 - + **description** *string*
 - + **match**
 - + **destination-address** *string*
 - + **destination-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **icmp6**
 - + **code** *number*
 - + **type** (*number | keyword*)
 - + **next-header** (*number | keyword*)
 - + **source-address** *string*
 - + **source-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **tcp-flags** *string*
 - **statistics**
 - **distributed-policer**
 - **conforming-octets** *number*
 - **conforming-packets** *number*
 - **exceeding-octets** *number*
 - **exceeding-packets** *number*
 - **last-clear** *string*
 - **last-match** *string*
 - **matched-packets** *number*
 - **system-cpu-policer**
 - **conforming-octets** *number*
 - **conforming-packets** *number*
 - **exceeding-octets** *number*
 - **exceeding-packets** *number*
 - **tcam-entries** *number*
 - **last-clear** *string*
 - + **statistics-per-entry** *boolean*
- + **ipv4-filter name** *string*

- + **description** *string*
 - + **entry sequence-id** *number*
 - + **action**
 - + **accept**
 - + **log** *boolean*
 - + **drop**
 - + **log** *boolean*
 - + **description** *string*
 - + **match**
 - + **destination-address** *string*
 - + **destination-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **first-fragment** *boolean*
 - + **fragment** *boolean*
 - + **icmp**
 - + **code** *number*
 - + **type** (*number | keyword*)
 - + **protocol** (*number | keyword*)
 - + **source-address** *string*
 - + **source-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **tcp-flags** *string*
 - **statistics**
 - **aggregate**
 - **in-last-match** *string*
 - **in-matched-packets** *number*
 - **out-last-match** *string*
 - **out-matched-packets** *number*
 - **last-clear** *string*
 - **per-interface**
 - **subinterface name** *string*
 - **in-last-match** *string*
 - **in-matched-packets** *number*
 - **last-clear** *string*
 - **out-last-match** *string*
 - **out-matched-packets** *number*
 - **tcam-entries**
 - **linecard slot** *number*
 - **input-total** *number*
 - **output-total** *number*
 - **single-instance** *number*
 - **last-clear** *string*
 - **statistics**
 - + **statistics-per-entry** *boolean*
 - + **subinterface-specific** *keyword*
- + **ipv6-filter name** *string*

- + **description** *string*
- + **entry sequence-id** *number*
- + **action**
 - + **accept**
 - + **log** *boolean*
 - + **drop**
 - + **log** *boolean*
- + **description** *string*
- + **match**
 - + **destination-address** *string*
 - + **destination-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **icmp6**
 - + **code** *number*
 - + **type** (*number | keyword*)
 - + **next-header** (*number | keyword*)
 - + **source-address** *string*
 - + **source-port**
 - + **operator** *keyword*
 - + **range**
 - + **end** (*number | keyword*)
 - + **start** (*number | keyword*)
 - + **value** (*number | keyword*)
 - + **tcp-flags** *string*
- **statistics**
 - **aggregate**
 - **in-last-match** *string*
 - **in-matched-packets** *number*
 - **out-last-match** *string*
 - **out-matched-packets** *number*
 - **last-clear** *string*
 - **per-interface**
 - **subinterface name** *string*
 - **in-last-match** *string*
 - **in-matched-packets** *number*
 - **last-clear** *string*
 - **out-last-match** *string*
 - **out-matched-packets** *number*
 - **tcam-entries**
 - **linecard slot** *number*
 - **input-total** *number*
 - **output-total** *number*
 - **single-instance** *number*
- **last-clear** *string*
- **statistics**
- + **statistics-per-entry** *boolean*
- + **subinterface-specific** *keyword*
- + **policers**
 - + **policer name** *string*
 - + **entry-specific** *boolean*

-
- + **max-burst** *number*
 - + **peak-rate** *number*
 - **statistics**
 - **conforming-octets** *number*
 - **conforming-packets** *number*
 - **exceeding-octets** *number*
 - **exceeding-packets** *number*
 - **last-clear** *string*
 - + **system-cpu-policer name** *string*
 - + **entry-specific** *boolean*
 - + **max-packet-burst** *number*
 - + **peak-packet-rate** *number*
 - **statistics**
 - **conforming-octets** *number*
 - **conforming-packets** *number*
 - **exceeding-octets** *number*
 - **exceeding-packets** *number*
 - **last-clear** *string*

2.1 acl Descriptions

acl

Context	acl
Tree	acl
Description	Top level container for configuration and operational state related to access control lists (ACLs)
Configurable	True

capture-filter

Context	acl capture-filter
Tree	capture-filter
Description	Top level container for capture filters
Configurable	True

ipv4-filter

Context	acl capture-filter ipv4-filter
Tree	ipv4-filter
Description	Top level container for capture IPv4 filters
Configurable	True

entry [sequence-id](#) *number*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

[sequence-id](#) *number*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Range	1 to 65535
Configurable	True

action

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> action
Tree	action
Description	Container for the actions to be applied to packets matching the capture filter entry.
Configurable	True

accept

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> action accept
Tree	accept
Description	Accept matching packets and forward them towards their normal destination
Configurable	True

copy

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> action copy
Tree	copy
Description	Create a copy of matching packets extract them to the CPM and deliver them to the designated veth interface
Configurable	True

description *string*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> description <i>string</i>
Tree	description
Description	Description string for the filter entry
String Length	1 to 255
Configurable	True

match

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match
Tree	match
Description	Container for the conditions that determine whether a packet matches this entry
Configurable	True

destination-address *string*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-address <i>string</i>
Tree	destination-address
Description	A packet matches this condition if its destination IP address is within the specified IPv4 prefix.
Configurable	True

destination-port

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port
Tree	destination-port
Description	A packet matches this condition if its destination TCP or UDP port number matches the value or range that is specified The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
Configurable	True

operator *keyword*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port operator <i>keyword</i>
Tree	operator
Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- `systat`
Active Users (`systat` service)
- `tacacs`
TACACS Login Host protocol
- `talk`
Talk
- `tcpmux`
TCP Port Service Multiplexer (TCPMUX)
- `tcpnethasprv`
`tcpnethasprv`, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context **acl capture-filter ipv4-filter entry sequence-id** *number match destination-port range start* (*number | keyword*)

Tree **start**

Description The starting port number to include in the range

Range 0 to 65535

Options

- `acap`
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetnetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl capture-filter ipv4-filter entry sequence-id** *number* **match destination-port value**
(*number | keyword*)

Tree **value**

Description A destination port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

first-fragment *boolean*

Context [acl capture-filter ipv4-filter entry sequence-id number match first-fragment](#) *boolean*

Tree [first-fragment](#)

Description Match the first fragment of an IPv4 datagram

A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and and the more-fragments bit is 1. It is not valid to configure this leaf without configuring a match value for the fragment leaf.

Configurable True

fragment *boolean*

Context [acl capture-filter ipv4-filter entry sequence-id number match fragment](#) *boolean*

Tree [fragment](#)

Description Match an IPv4 fragment

A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and and the more-fragments bit is 1 or if the IPv4 header indicates that the fragment-offset is greater than 0. A packet matches the false condition if it is unfragmented.

Configurable True

icmp

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match icmp
Tree	icmp
Description	<p>A packet matches this condition if its ICMP type and code matches one of the specified combinations</p> <p>The rule should also have a condition that the IP protocol equals 1 (ICMP) in order for this to be interpreted correctly.</p>
Configurable	True

code *number*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match icmp code <i>number</i>
Tree	code
Description	<p>Match if the ICMP code value is any value in the list</p> <p>Requires ICMP type to be specified because codes are type dependent.</p>
Configurable	True

type (*number* | *keyword*)

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match icmp type (<i>number</i> <i>keyword</i>)
Tree	type
Description	Match a single ICMP type value.
Range	0 to 255
Options	<ul style="list-style-type: none">• echo-reply ICMP Echo Reply• dest-unreachable ICMP Destination Unreachable• source-quench ICMP Source Quench• redirect ICMP Redirect• echo ICMP Echo• router-advertise ICMP Router Advertisement• router-solicit ICMP Router Solicitation

	<ul style="list-style-type: none">• time-exceeded ICMP Time Exceeded• param-problem ICMP Parameter Problem• timestamp ICMP Timestamp• timestamp-reply ICMP Timestamp Reply
Configurable	True

protocol (*number | keyword*)

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match protocol (<i>number keyword</i>)
Tree	protocol
Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Range	0 to 255
Options	<ul style="list-style-type: none">• ipv6-hop IPv6 hop-by-hop option• icmp Internet Control Message Protocol• igmp Internet Group Management Protocol• ggp Gateway-to-Gateway Protocol• ipv4 IPv4 encapsulation• st Stream Protocol• tcp Transmission Control Protocol• egp Exterior Gateway Protocol• igp Interior Gateway Protocol• udp User Datagram Protocol• ipv6 IPv6 encapsulation

- idrp
Inter-Domain Routing Protocol
- rsvp
Resource Reservation Protocol
- gre
Generic Routing Encapsulation
- esp
IPSec Encapsulating Security Payload
- ah
IPSec Authentication Header
- icmp6
IPSec Authentication Header
- no-next-hdr
No Next Header for IPv6
- ipv6-dest-opts
Destination Options for IPv6
- eigrp
Cisco EIGRP
- pim
Protocol Independent Multicast
- vrrp
Virtual Router Redundancy Protocol
- l2tp
Layer Two Tunneling Protocol
- sctp
Stream Control Transmission Protocol
- mpls-in-ip
MPLS Encapsulation inside IP
- rohc
Robust Header Compression

Configurable True

source-address *string*

Context **acl capture-filter ipv4-filter entry sequence-id** *number match source-address string*

Tree **source-address**

Description A packet matches this condition if its source IP address is within the specified IPv4 prefix

Configurable True

source-port

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port
Tree	source-port
Description	<p>A packet matches this condition if its source TCP or UDP port number matches the value or range that is specified</p> <p>The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.</p>
Configurable	True

operator *keyword*

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port operator <i>keyword</i>
Tree	operator
Description	<p>Comparison operator</p> <p>eq = equal ge = greater than or equal to le = less than or equal to</p>
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- `systat`
Active Users (`systat` service)
- `tacacs`
TACACS Login Host protocol
- `talk`
Talk
- `tcpmux`
TCP Port Service Multiplexer (TCPMUX)
- `tcpnethasprv`
`tcpnethasprv`, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context **acl capture-filter ipv4-filter entry sequence-id** *number match source-port range start*
(*number | keyword*)

Tree **start**

Description The starting port number to include in the range

Range 0 to 65535

Options

- `acap`
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl capture-filter ipv4-filter entry sequence-id number match source-port value** (*number | keyword*)

Tree **value**

Description A source port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

tcp-flags *string*

Context [acl capture-filter ipv4-filter entry sequence-id number match tcp-flags string](#)

Tree [tcp-flags](#)

Description A logical expression using the &, | and ! logical operators and the TCP flag names: rst, syn and ack.

Configurable True

tcam-entries *number*

Context [acl capture-filter ipv4-filter entry sequence-id number tcam-entries number](#)

Tree [tcam-entries](#)

Description The number of TCAM entries required to implement a single instance of this filter rule.

Configurable False

ipv6-filter

Context [acl capture-filter ipv6-filter](#)

Tree [ipv6-filter](#)

Description Top level container for capture IPv6 filters

Configurable True

entry **sequence-id** *number*

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Range	1 to 65535
Configurable	True

action

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> action
Tree	action
Description	Container for the actions to be applied to packets matching the capture filter entry.
Configurable	True

accept

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> action accept
Tree	accept
Description	Accept matching packets and forward them towards their normal destination
Configurable	True

copy

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> action copy
Tree	copy
Description	Create a copy of matching packets extract them to the CPM and deliver them to the designated veth interface
Configurable	True

description *string*

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> description <i>string</i>
Tree	description
Description	Description string for the filter entry
String Length	1 to 255
Configurable	True

match

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match
Tree	match
Description	Container for the conditions that determine whether a packet matches this entry
Configurable	True

destination-address *string*

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-address <i>string</i>
Tree	destination-address
Description	A packet matches this condition if its destination IP address is within the specified IPv6 prefix
Configurable	True

destination-port

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port
Tree	destination-port
Description	A packet matches this condition if its destination TCP or UDP port number matches the value or range that is specified The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
Configurable	True

operator *keyword*

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port operator <i>keyword</i>
Tree	operator
Description	Comparison operator

	eq = equal ge = greater than or equal to le = less than or equal to
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number* | *keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth

-
- Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine

-
- discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname

-
- NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol

-
- kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor

-
- Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who

-
- nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct

-
- RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps

-
- snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch

	Xerox Network Systems (XNS) Clearinghouse (Name Server)
	• xns-mail Xerox Network Systems (XNS) Mail
	• xns-time Xerox Network Systems (XNS) Time Protocol
	• z3950 ANSI Z39.50
Configurable	True

start (*number | keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range start (<i>number keyword</i>)
Tree	start
Description	The starting port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp

-
- Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol

-
- echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt

-
- http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password

-
- kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp

-
- Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)

-
- odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip

-
- Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service

-
- ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
 - xns-mail
Xerox Network Systems (XNS) Mail
 - xns-time
Xerox Network Systems (XNS) Time Protocol
 - z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port value (<i>number keyword</i>)
Tree	value
Description	A destination port number
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- **systat**
Active Users (systat service)
- **tacacs**
TACACS Login Host protocol
- **talk**
Talk
- **tcpmux**
TCP Port Service Multiplexer (TCPMUX)
- **tcpnethasprv**
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- **tftp**
Trivial File Transfer Protocol (TFTP)
- **time**
Time Protocol
- **timed**
Timeserver
- **ups**
Uninterruptible power supply (UPS)
- **xdmcp**
X Display Manager Control Protocol (XDMCP)
- **xns-ch**
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- **xns-mail**
Xerox Network Systems (XNS) Mail
- **xns-time**
Xerox Network Systems (XNS) Time Protocol
- **z3950**
ANSI Z39.50

Configurable True

icmp6

Context [acl capture-filter ipv6-filter entry sequence-id number match icmp6](#)

Tree [icmp6](#)

Description A packet matches this condition if its ICMPv6 type and code matches one of the specified combinations

The rule should also have a condition that the next-header value equals 58 (ICMPv6) in order for this to be interpreted correctly.

Configurable True

code *number*

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match icmp6 code <i>number</i>
Tree	code
Description	Match if the ICMPv6 code value is any value in the list Requires ICMPv6 type to be specified because codes are type dependent.
Configurable	True

type (*number | keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match icmp6 type (<i>number keyword</i>)
Tree	type
Description	Match a single ICMPv6 type value
Range	0 to 255
Options	<ul style="list-style-type: none">• <code>dest-unreachable</code> ICMPv6 Destination Unreachable• <code>packet-too-big</code> ICMPv6 Packet Too Big• <code>time-exceeded</code> ICMPv6 Time Exceeded• <code>param-problem</code> Parameter Problem• <code>echo-request</code> ICMPv6 Echo Request• <code>echo-reply</code> ICMPv6 Echo Reply• <code>mld-query</code> Multicast Listener Discovery Query• <code>mld-report</code> Multicast Listener Discovery Report• <code>mld-done</code> Multicast Listener Discovery Done• <code>router-solicit</code> ICMPv6 Router Solicitation• <code>router-advertise</code> ICMPv6 Router Advertisement• <code>neighbor-solicit</code> ICMPv6 Neighbor Solicitation

- neighbor-advertise
ICMPv6 Neighbor Advertisement
- redirect
ICMPv6 Redirect
- router-renumber
ICMPv6 Router Renumbering
- node-info-query
ICMPv6 Node Information Query
- node-info-response
ICMPv6 Node Information Response
- mld-v2
Multicast Listener Discovery Version 2
- mcast-rtr-adv
Multicast Router Advertisement
- mcast-rtr-solicit
Multicast Router Solicitation
- mcast-rtr-term
Multicast Router Termination

Configurable True

next-header (*number | keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number match next-header</i> (<i>number keyword</i>)
Tree	next-header
Description	An IPv6 packet matches this condition if its first next-header field (in the IPv6 fixed header) contains the specified value
Range	0 to 255
Options	<ul style="list-style-type: none">• ipv6-hop IPv6 hop-by-hop option• icmp Internet Control Message Protocol• igmp Internet Group Management Protocol• ggp Gateway-to-Gateway Protocol• ipv4 IPv4 encapsulation• st

-
- Stream Protocol
 - tcp
Transmission Control Protocol
 - egp
Exterior Gateway Protocol
 - igp
Interior Gateway Protocol
 - udp
User Datagram Protocol
 - ipv6
IPv6 encapsulation
 - idrp
Inter-Domain Routing Protocol
 - rsvp
Resource Reservation Protocol
 - gre
Generic Routing Encapsulation
 - esp
IPSec Encapsulating Security Payload
 - ah
IPSec Authentication Header
 - icmp6
IPSec Authentication Header
 - no-next-hdr
No Next Header for IPv6
 - ipv6-dest-opts
Destination Options for IPv6
 - eigrp
Cisco EIGRP
 - pim
Protocol Independent Multicast
 - vrrp
Virtual Router Redundancy Protocol
 - l2tp
Layer Two Tunneling Protocol
 - sctp
Stream Control Transmission Protocol
 - mpls-in-ip
MPLS Encapsulation inside IP

- rohc
Robust Header Compression
- Configurable True

source-address *string*

- Context [acl capture-filter ipv6-filter entry sequence-id number match source-address string](#)
- Tree [source-address](#)
- Description A packet matches this condition if its source IP address is within the specified IPv6 prefix
- Configurable True

source-port

- Context [acl capture-filter ipv6-filter entry sequence-id number match source-port](#)
- Tree [source-port](#)
- Description A packet matches this condition if its source TCP or UDP port number matches the value or range that is specified
- The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
- Configurable True

operator *keyword*

- Context [acl capture-filter ipv6-filter entry sequence-id number match source-port operator keyword](#)
- Tree [operator](#)
- Description Comparison operator
- eq = equal ge = greater than or equal to le = less than or equal to
- Options
- le
Less than or equal.
 - ge
Greater than or equal.
 - eq
Equal to.
- Configurable True

range

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match source-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number* | *keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• <code>acap</code> Application Configuration Access Protocol• <code>afp-tcp</code> Apple Filing Protocol over TCP• <code>arns</code> A Remote Network Server System• <code>asf-rmcp</code> ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• <code>ashare</code> AppleShare IP Web Administration• <code>atalk-rm</code> AppleTalk Routing Maintenance• <code>aurp</code> AppleTalk Update-Based Routing Protocol• <code>auth</code> Authentication Service• <code>bfd</code> Bidirectional Forwarding Detection Single Hop• <code>bfd-echo</code> BFD Echo• <code>bftp</code> Background File Transfer Program• <code>bgmp</code> Border Gateway Multicast Protocol• <code>bgp</code>

-
- Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol

-
- epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc

-
- Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell

-
- l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange

-
- MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)

-
- olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje

-
- Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol

-
- submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
 - xns-mail
Xerox Network Systems (XNS) Mail
 - xns-time
Xerox Network Systems (XNS) Time Protocol
 - z3950
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match source-port range start (<i>number keyword</i>)
Tree	start
Description	The starting port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- **systat**
Active Users (systat service)
- **tacacs**
TACACS Login Host protocol
- **talk**
Talk
- **tcpmux**
TCP Port Service Multiplexer (TCPMUX)
- **tcpnethasprv**
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- **tftp**
Trivial File Transfer Protocol (TFTP)
- **time**
Time Protocol
- **timed**
Timeserver
- **ups**
Uninterruptible power supply (UPS)
- **xdmcp**
X Display Manager Control Protocol (XDMCP)
- **xns-ch**
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- **xns-mail**
Xerox Network Systems (XNS) Mail
- **xns-time**
Xerox Network Systems (XNS) Time Protocol
- **z3950**
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl capture-filter ipv6-filter entry sequence-id number match source-port value** (*number | keyword*)

Tree **value**

Description A source port number

Range 0 to 65535

Options

- **acap**
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetnetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- `tcpnethasprv`
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

tcp-flags *string*

Context [acl capture-filter ipv6-filter entry sequence-id number match tcp-flags string](#)

Tree [tcp-flags](#)

Description A logical expression using the &, | and ! logical operators and the TCP flag names: rst, syn and ack.

Configurable True

tcam-entries *number*

Context [acl capture-filter ipv6-filter entry sequence-id number tcam-entries number](#)

Tree [tcam-entries](#)

Description The number of TCAM entries required to implement a single instance of this filter rule.

Configurable False

cpm-filter

Context	acl cpm-filter
Tree	cpm-filter
Description	Top level container for CPM filters
Configurable	True

ipv4-filter

Context	acl cpm-filter ipv4-filter
Tree	ipv4-filter
Description	Top level container for CPM IPv4 filters
Configurable	True

entry [sequence-id](#) *number*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

[sequence-id](#) *number*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Range	1 to 65535
Configurable	True

action

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action
Tree	action
Description	Container for the actions to be applied to packets matching the CPM filter entry.
Configurable	True

accept

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action accept
Tree	accept
Description	Accept matching packets and forward them towards their normal destination
Configurable	True

log *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action accept log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: <ul style="list-style-type: none">• timestamp• filter name• filter entry sequence-id• incoming linecard• action: accept• IP protocol• packet-length• source-IP• source-port (TCP/UDP packets)• dest-IP• dest-port (TCP/UDP packets)• icmp-type (ICMP packets)• icmp-code (ICMP packets)
Default	false
Configurable	True

rate-limit

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action accept rate-limit
Tree	rate-limit
Description	Rate-limit accepted packets
Configurable	True

distributed-policer *reference*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action accept rate-limit distributed-policer <i>reference</i>
Tree	distributed-policer
Description	Reference to a policer
Reference	acl policers policer name <i>string</i>
Configurable	True

system-cpu-policer *reference*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action accept rate-limit system-cpu-policer <i>reference</i>
Tree	system-cpu-policer
Description	Reference to a system-cpu-policer.
Reference	acl policers system-cpu-policer name <i>string</i>
Configurable	True

drop

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action drop
Tree	drop
Description	Drop matching packets without sending any ICMP messages back to the source
Configurable	True

log *boolean*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> action drop log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:

- timestamp
- filter name
- filter entry sequence-id
- incoming linecard
- action: drop
- IP protocol
- packet-length
- source-IP
- source-port (TCP/UDP packets)
- dest-IP
- dest-port (TCP/UDP packets)
- icmp-type (ICMP packets)
- icmp-code (ICMP packets)

Default false
Configurable True

description *string*

Context [acl cpm-filter ipv4-filter entry sequence-id](#) *number* [description](#) *string*
Tree [description](#)
Description Description string for the filter entry
String Length 1 to 255
Configurable True

match

Context [acl cpm-filter ipv4-filter entry sequence-id](#) *number* [match](#)
Tree [match](#)
Description Container for the conditions that determine whether a packet matches this entry
Configurable True

destination-address *string*

Context [acl cpm-filter ipv4-filter entry sequence-id](#) *number* [match destination-address](#) *string*
Tree [destination-address](#)
Description A packet matches this condition if its destination IP address is within the specified IPv4 prefix.
Configurable True

destination-port

Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-port
Tree	destination-port
Description	A packet matches this condition if its destination TCP or UDP port number matches the value or range that is specified The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
Configurable	True

operator *keyword*

Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-port operator keyword
Tree	operator
Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- **systat**
Active Users (systat service)
- **tacacs**
TACACS Login Host protocol
- **talk**
Talk
- **tcpmux**
TCP Port Service Multiplexer (TCPMUX)
- **tcpnethasprv**
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- **tftp**
Trivial File Transfer Protocol (TFTP)
- **time**
Time Protocol
- **timed**
Timeserver
- **ups**
Uninterruptible power supply (UPS)
- **xdmcp**
X Display Manager Control Protocol (XDMCP)
- **xns-ch**
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- **xns-mail**
Xerox Network Systems (XNS) Mail
- **xns-time**
Xerox Network Systems (XNS) Time Protocol
- **z3950**
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context **acl cpm-filter ipv4-filter entry sequence-id number match destination-port range start**
(*number | keyword*)

Tree **start**

Description The starting port number to include in the range

Range 0 to 65535

Options

- **acap**
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl cpm-filter ipv4-filter entry sequence-id number match destination-port value**
(*number | keyword*)

Tree **value**

Description A destination port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

first-fragment *boolean*

Context [acl cpm-filter ipv4-filter entry sequence-id number match first-fragment](#) *boolean*

Tree [first-fragment](#)

Description Match the first fragment of an IPv4 datagram

A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and and the more-fragments bit is 1. It is not valid to configure this leaf without configuring a match value for the fragment leaf.

Configurable True

fragment *boolean*

Context [acl cpm-filter ipv4-filter entry sequence-id number match fragment](#) *boolean*

Tree [fragment](#)

Description Match an IPv4 fragment

A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and and the more-fragments bit is 1 or if the IPv4 header indicates that the fragment-offset is greater than 0. A packet matches the false condition if it is unfragmented.

Configurable True

icmp

Context	acl cpm-filter ipv4-filter entry sequence-id number match icmp
Tree	icmp
Description	A packet matches this condition if its ICMP type and code matches one of the specified combinations The rule should also have a condition that the IP protocol equals 1 (ICMP) in order for this to be interpreted correctly.
Configurable	True

code *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number match icmp code number
Tree	code
Description	Match if the ICMP code value is any value in the list Requires ICMP type to be specified because codes are type dependent.
Configurable	True

type (*number* | *keyword*)

Context	acl cpm-filter ipv4-filter entry sequence-id number match icmp type (<i>number</i> <i>keyword</i>)
Tree	type
Description	Match a single ICMP type value.
Range	0 to 255
Options	<ul style="list-style-type: none">• echo-reply ICMP Echo Reply• dest-unreachable ICMP Destination Unreachable• source-quench ICMP Source Quench• redirect ICMP Redirect• echo ICMP Echo• router-advertise ICMP Router Advertisement• router-solicit ICMP Router Solicitation• time-exceeded

	ICMP Time Exceeded
	• param-problem
	ICMP Parameter Problem
	• timestamp
	ICMP Timestamp
	• timestamp-reply
	ICMP Timestamp Reply
Configurable	True

protocol (*number | keyword*)

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match protocol (<i>number keyword</i>)
Tree	protocol
Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Range	0 to 255
Options	<ul style="list-style-type: none">• ipv6-hop IPv6 hop-by-hop option• icmp Internet Control Message Protocol• igmp Internet Group Management Protocol• ggp Gateway-to-Gateway Protocol• ipv4 IPv4 encapsulation• st Stream Protocol• tcp Transmission Control Protocol• egp Exterior Gateway Protocol• igp Interior Gateway Protocol• udp User Datagram Protocol• ipv6 IPv6 encapsulation• idrp Inter-Domain Routing Protocol

- rsvp
Resource Reservation Protocol
- gre
Generic Routing Encapsulation
- esp
IPSec Encapsulating Security Payload
- ah
IPSec Authentication Header
- icmp6
IPSec Authentication Header
- no-next-hdr
No Next Header for IPv6
- ipv6-dest-opts
Destination Options for IPv6
- eigrp
Cisco EIGRP
- pim
Protocol Independent Multicast
- vrrp
Virtual Router Redundancy Protocol
- l2tp
Layer Two Tunneling Protocol
- sctp
Stream Control Transmission Protocol
- mpls-in-ip
MPLS Encapsulation inside IP
- rohc
Robust Header Compression

Configurable True

source-address *string*

Context **acl cpm-filter ipv4-filter entry sequence-id number match source-address** *string*

Tree **source-address**

Description A packet matches this condition if its source IP address is within the specified IPv4 prefix

Configurable True

source-port

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match source-port
Tree	source-port
Description	<p>A packet matches this condition if its source TCP or UDP port number matches the value or range that is specified</p> <p>The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.</p>
Configurable	True

operator *keyword*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match source-port operator <i>keyword</i>
Tree	operator
Description	<p>Comparison operator</p> <p>eq = equal ge = greater than or equal to le = less than or equal to</p>
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match source-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match source-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- `systat`
Active Users (`systat` service)
- `tacacs`
TACACS Login Host protocol
- `talk`
Talk
- `tcpmux`
TCP Port Service Multiplexer (TCPMUX)
- `tcpnethasprv`
`tcpnethasprv`, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number match source-port range start</i> (<i>number keyword</i>)
Tree	start
Description	The starting port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• <code>acap</code> Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
 - Remote Procedure Call
 - daytime
 - Daytime Protocol
 - dhcpv6-client
 - DHCPv6 Client
 - dhcpv6-server
 - DHCPv6 Server
 - dhcp-failover
 - DHCP Failover Protocol
 - dicom
 - Digital Imaging and Communications in Medicine
 - discard
 - Discard Protocol. Also Wake-on-LAN.
 - dnsix
 - DNSIX security protocol auditing
 - domain
 - Domain Name System
 - dsp
 - Display Support Protocol
 - echo
 - Echo Protocol
 - epp
 - Extensible Provisioning Protocol
 - esro
 - Efficient Short Remote Operations (ESRO)
 - exec
 - Remote Process Execution (Rexec)
 - finger
 - Finger protocol
 - ftp
 - File Transfer Protocol control
 - ftp-data
 - File Transfer Protocol data
 - ftps
 - FTPS (FTP over SSL/TLS) control
 - ftps-data
 - FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl cpm-filter ipv4-filter entry sequence-id number match source-port value** (*number | keyword*)

Tree **value**

Description A source port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

tcp-flags *string*

Context [acl cpm-filter ipv4-filter entry sequence-id number match tcp-flags string](#)

Tree [tcp-flags](#)

Description A logical expression using the &, | and ! logical operators and the TCP flag names: rst, syn and ack.

Configurable True

statistics

Context [acl cpm-filter ipv4-filter entry sequence-id number statistics](#)

Tree [statistics](#)

Description Statistics container for packets matching the CPM-filter entry

Configurable False

distributed-policer

Context [acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer](#)

Tree [distributed-policer](#)

Description Distributed policer stats for traffic matching the entry.

Configurable False

conforming-octets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer conforming-octets number
Tree	conforming-octets
Description	The number of bytes that were considered conforming by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

conforming-packets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer conforming-packets number
Tree	conforming-packets
Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Default	0
Configurable	False

exceeding-octets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer exceeding-octets number
Tree	exceeding-octets
Description	The number of bytes that were considered exceeding by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

exceeding-packets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer exceeding-packets number
Tree	exceeding-packets
Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Default	0
Configurable	False

last-clear *string*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level
Configurable	False

last-match *string*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics last-match <i>string</i>
Tree	last-match
Description	The elapsed time since a packet last matched the entry, considering all subinterfaces and all linecards.
Configurable	False

matched-packets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics matched-packets <i>number</i>
Tree	matched-packets
Description	The number of packets matching the entry since it was programmed or since the last clear, summed across all subinterfaces and all linecards
Default	0
Configurable	False

system-cpu-policer

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics system-cpu-policer
Tree	system-cpu-policer
Description	System CPU policer stats for traffic matching the entry.
Configurable	False

conforming-octets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer conforming-octets number
Tree	conforming-octets
Description	The number of bytes that were considered conforming by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

conforming-packets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer conforming-packets number
Tree	conforming-packets
Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Default	0
Configurable	False

exceeding-octets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer exceeding-octets number
Tree	exceeding-octets
Description	The number of bytes that were considered exceeding by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

exceeding-packets *number*

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer exceeding-packets number
Tree	exceeding-packets
Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Default	0
Configurable	False

tcam-entries *number*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> tcam-entries <i>number</i>
Tree	tcam-entries
Description	The number of TCAM entries required to implement a single instance of this filter rule.
Configurable	False

last-clear *string*

Context	acl cpm-filter ipv4-filter last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level
Configurable	False

statistics-per-entry *boolean*

Context	acl cpm-filter ipv4-filter statistics-per-entry <i>boolean</i>
Tree	statistics-per-entry
Description	Collect the following statistics per entry: the number of packets matching each entry, and the elapsed time since a packet last matched each entry
Configurable	True

ipv6-filter

Context	acl cpm-filter ipv6-filter
Tree	ipv6-filter
Description	Top level container for CPM IPv6 filters
Configurable	True

entry [sequence-id](#) *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Range	1 to 65535
Configurable	True

action

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> action
Tree	action
Description	Container for the actions to be applied to packets matching the CPM filter entry.
Configurable	True

accept

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> action accept
Tree	accept
Description	Accept matching packets and forward them towards their normal destination
Configurable	True

log *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> action accept log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: <ul style="list-style-type: none">• timestamp• filter name• filter entry sequence-id• incoming linecard• action: accept• IP protocol

	<ul style="list-style-type: none">• packet-length• source-IP• source-port (TCP/UDP packets)• dest-IP• dest-port (TCP/UDP packets)• icmp-type (ICMP packets)• icmp-code (ICMP packets)
Default	false
Configurable	True

rate-limit

Context	acl cpm-filter ipv6-filter entry sequence-id number action accept rate-limit
Tree	rate-limit
Description	Rate-limit accepted packets
Configurable	True

distributed-policer *reference*

Context	acl cpm-filter ipv6-filter entry sequence-id number action accept rate-limit distributed-policer reference
Tree	distributed-policer
Description	Reference to a policer
Reference	acl policers policer name string
Configurable	True

system-cpu-policer *reference*

Context	acl cpm-filter ipv6-filter entry sequence-id number action accept rate-limit system-cpu-policer reference
Tree	system-cpu-policer
Description	Reference to a system-cpu-policer.
Reference	acl policers system-cpu-policer name string
Configurable	True

drop

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> action drop
Tree	drop
Description	Drop matching packets without sending any ICMP messages back to the source
Configurable	True

log *boolean*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> action drop log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: <ul style="list-style-type: none">• timestamp• filter name• filter entry sequence-id• incoming linecard• action: drop• IP protocol• packet-length• source-IP• source-port (TCP/UDP packets)• dest-IP• dest-port (TCP/UDP packets)• icmp-type (ICMP packets)• icmp-code (ICMP packets)
Default	false
Configurable	True

description *string*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> description <i>string</i>
Tree	description
Description	Description string for the filter entry
String Length	1 to 255
Configurable	True

match

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match
Tree	match
Description	Container for the conditions that determine whether a packet matches this entry
Configurable	True

destination-address *string*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-address <i>string</i>
Tree	destination-address
Description	A packet matches this condition if its destination IP address is within the specified IPv6 prefix
Configurable	True

destination-port

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port
Tree	destination-port
Description	<p>A packet matches this condition if its destination TCP or UDP port number matches the value or range that is specified</p> <p>The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.</p>
Configurable	True

operator *keyword*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port operator <i>keyword</i>
Tree	operator
Description	<p>Comparison operator</p> <p>eq = equal ge = greater than or equal to le = less than or equal to</p>
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number* | *keyword*)

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp

-
- Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol

-
- epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc

-
- Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell

-
- l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange

-
- MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)

-
- olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje

-
- Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol

-
- submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
 - xns-mail
Xerox Network Systems (XNS) Mail
 - xns-time
Xerox Network Systems (XNS) Time Protocol
 - z3950
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range start (<i>number keyword</i>)
Tree	start
Description	The starting port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- **systat**
Active Users (systat service)
- **tacacs**
TACACS Login Host protocol
- **talk**
Talk
- **tcpmux**
TCP Port Service Multiplexer (TCPMUX)
- **tcpnethasprv**
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- **tftp**
Trivial File Transfer Protocol (TFTP)
- **time**
Time Protocol
- **timed**
Timeserver
- **ups**
Uninterruptible power supply (UPS)
- **xdmcp**
X Display Manager Control Protocol (XDMCP)
- **xns-ch**
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- **xns-mail**
Xerox Network Systems (XNS) Mail
- **xns-time**
Xerox Network Systems (XNS) Time Protocol
- **z3950**
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl cpm-filter ipv6-filter entry sequence-id number match destination-port value**
(*number | keyword*)

Tree **value**

Description A destination port number

Range 0 to 65535

Options

- **acap**
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
 - Remote Procedure Call
 - daytime
 - Daytime Protocol
 - dhcpv6-client
 - DHCPv6 Client
 - dhcpv6-server
 - DHCPv6 Server
 - dhcp-failover
 - DHCP Failover Protocol
 - dicom
 - Digital Imaging and Communications in Medicine
 - discard
 - Discard Protocol. Also Wake-on-LAN.
 - dnsix
 - DNSIX security protocol auditing
 - domain
 - Domain Name System
 - dsp
 - Display Support Protocol
 - echo
 - Echo Protocol
 - epp
 - Extensible Provisioning Protocol
 - esro
 - Efficient Short Remote Operations (ESRO)
 - exec
 - Remote Process Execution (Rexec)
 - finger
 - Finger protocol
 - ftp
 - File Transfer Protocol control
 - ftp-data
 - File Transfer Protocol data
 - ftps
 - FTPS (FTP over SSL/TLS) control
 - ftps-data
 - FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetnetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- `tcpnethasprv`
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

icmp6

Context [acl cpm-filter ipv6-filter entry sequence-id number match icmp6](#)

Tree [icmp6](#)

Description A packet matches this condition if its ICMPv6 type and code matches one of the specified combinations

The rule should also have a condition that the next-header value equals 58 (ICMPv6) in order for this to be interpreted correctly.

Configurable True

code number

Context [acl cpm-filter ipv6-filter entry sequence-id number match icmp6 code number](#)

Tree [code](#)

Description Match if the ICMPv6 code value is any value in the list

Requires ICMPv6 type to be specified because codes are type dependent.

Configurable True

type (*number | keyword*)

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match icmp6 type (<i>number keyword</i>)
Tree	type
Description	Match a single ICMPv6 type value
Range	0 to 255
Options	<ul style="list-style-type: none">• dest-unreachable ICMPv6 Destination Unreachable• packet-too-big ICMPv6 Packet Too Big• time-exceeded ICMPv6 Time Exceeded• param-problem Parameter Problem• echo-request ICMPv6 Echo Request• echo-reply ICMPv6 Echo Reply• mld-query Multicast Listener Discovery Query• mld-report Multicast Listener Discovery Report• mld-done Multicast Listener Discovery Done• router-solicit ICMPv6 Router Solicitation• router-advertise ICMPv6 Router Advertisement• neighbor-solicit ICMPv6 Neighbor Solicitation• neighbor-advertise ICMPv6 Neighbor Advertisement• redirect ICMPv6 Redirect• router-renomber ICMPv6 Router Renumbering• node-info-query ICMPv6 Node Information Query• node-info-response

	ICMPv6 Node Information Response
	• mld-v2
	Multicast Listener Discovery Version 2
	• mcast-rtr-adv
	Multicast Router Advertisement
	• mcast-rtr-solicit
	Multicast Router Solicitation
	• mcast-rtr-term
	Multicast Router Termination
Configurable	True

next-header (*number | keyword*)

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match next-header (<i>number keyword</i>)
Tree	next-header
Description	An IPv6 packet matches this condition if its first next-header field (in the IPv6 fixed header) contains the specified value
Range	0 to 255
Options	<ul style="list-style-type: none">• ipv6-hop IPv6 hop-by-hop option• icmp Internet Control Message Protocol• igmp Internet Group Management Protocol• ggp Gateway-to-Gateway Protocol• ipv4 IPv4 encapsulation• st Stream Protocol• tcp Transmission Control Protocol• egp Exterior Gateway Protocol• igp Interior Gateway Protocol• udp User Datagram Protocol

-
- ipv6
IPv6 encapsulation
 - idrp
Inter-Domain Routing Protocol
 - rsvp
Resource Reservation Protocol
 - gre
Generic Routing Encapsulation
 - esp
IPSec Encapsulating Security Payload
 - ah
IPSec Authentication Header
 - icmp6
IPSec Authentication Header
 - no-next-hdr
No Next Header for IPv6
 - ipv6-dest-opts
Destination Options for IPv6
 - eigrp
Cisco EIGRP
 - pim
Protocol Independent Multicast
 - vrrp
Virtual Router Redundancy Protocol
 - l2tp
Layer Two Tunneling Protocol
 - sctp
Stream Control Transmission Protocol
 - mpls-in-ip
MPLS Encapsulation inside IP
 - rohc
Robust Header Compression

Configurable True

source-address *string*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-address <i>string</i>
Tree	source-address
Description	A packet matches this condition if its source IP address is within the specified IPv6 prefix
Configurable	True

source-port

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port
Tree	source-port
Description	A packet matches this condition if its source TCP or UDP port number matches the value or range that is specified The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
Configurable	True

operator *keyword*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port operator <i>keyword</i>
Tree	operator
Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- `systat`
Active Users (`systat` service)
- `tacacs`
TACACS Login Host protocol
- `talk`
Talk
- `tcpmux`
TCP Port Service Multiplexer (TCPMUX)
- `tcpnethasprv`
`tcpnethasprv`, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context **acl cpm-filter ipv6-filter entry sequence-id number match source-port range start**
(*number | keyword*)

Tree **start**

Description The starting port number to include in the range

Range 0 to 65535

Options

- `acap`
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
 - Remote Procedure Call
 - daytime
 - Daytime Protocol
 - dhcpv6-client
 - DHCPv6 Client
 - dhcpv6-server
 - DHCPv6 Server
 - dhcp-failover
 - DHCP Failover Protocol
 - dicom
 - Digital Imaging and Communications in Medicine
 - discard
 - Discard Protocol. Also Wake-on-LAN.
 - dnsix
 - DNSIX security protocol auditing
 - domain
 - Domain Name System
 - dsp
 - Display Support Protocol
 - echo
 - Echo Protocol
 - epp
 - Extensible Provisioning Protocol
 - esro
 - Efficient Short Remote Operations (ESRO)
 - exec
 - Remote Process Execution (Rexec)
 - finger
 - Finger protocol
 - ftp
 - File Transfer Protocol control
 - ftp-data
 - File Transfer Protocol data
 - ftps
 - FTPS (FTP over SSL/TLS) control
 - ftps-data
 - FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetnetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl cpm-filter ipv6-filter entry sequence-id number match source-port value** (*number | keyword*)

Tree **value**

Description A source port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

tcp-flags *string*

Context [acl cpm-filter ipv6-filter entry sequence-id number match tcp-flags string](#)

Tree [tcp-flags](#)

Description A logical expression using the &, | and ! logical operators and the TCP flag names: rst, syn and ack.

Configurable True

statistics

Context [acl cpm-filter ipv6-filter entry sequence-id number statistics](#)

Tree [statistics](#)

Description Statistics container for packets matching the CPM-filter entry

Configurable False

distributed-policer

Context [acl cpm-filter ipv6-filter entry sequence-id number statistics distributed-policer](#)

Tree [distributed-policer](#)

Description Distributed policer stats for traffic matching the entry.

Configurable False

conforming-octets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id number statistics distributed-policer conforming-octets number
Tree	conforming-octets
Description	The number of bytes that were considered conforming by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

conforming-packets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id number statistics distributed-policer conforming-packets number
Tree	conforming-packets
Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Default	0
Configurable	False

exceeding-octets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id number statistics distributed-policer exceeding-octets number
Tree	exceeding-octets
Description	The number of bytes that were considered exceeding by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

exceeding-packets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id number statistics distributed-policer exceeding-packets number
Tree	exceeding-packets
Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Default	0
Configurable	False

last-clear *string*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level
Configurable	False

last-match *string*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics last-match <i>string</i>
Tree	last-match
Description	The elapsed time since a packet last matched the entry, considering all subinterfaces and all linecards.
Configurable	False

matched-packets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics matched-packets <i>number</i>
Tree	matched-packets
Description	The number of packets matching the entry since it was programmed or since the last clear, summed across all subinterfaces and all linecards
Default	0
Configurable	False

system-cpu-policer

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics system-cpu-policer
Tree	system-cpu-policer
Description	System CPU policer stats for traffic matching the entry.
Configurable	False

conforming-octets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics system-cpu-policer conforming-octets <i>number</i>
Tree	conforming-octets
Description	The number of bytes that were considered conforming by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

conforming-packets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics system-cpu-policer conforming-packets <i>number</i>
Tree	conforming-packets
Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Default	0
Configurable	False

exceeding-octets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics system-cpu-policer exceeding-octets <i>number</i>
Tree	exceeding-octets
Description	The number of bytes that were considered exceeding by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

exceeding-packets *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics system-cpu-policer exceeding-packets <i>number</i>
Tree	exceeding-packets
Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Default	0
Configurable	False

tcam-entries *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> tcam-entries <i>number</i>
Tree	tcam-entries
Description	The number of TCAM entries required to implement a single instance of this filter rule.
Configurable	False

last-clear *string*

Context	acl cpm-filter ipv6-filter last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level
Configurable	False

statistics-per-entry *boolean*

Context	acl cpm-filter ipv6-filter statistics-per-entry <i>boolean</i>
Tree	statistics-per-entry
Description	Collect the following statistics per entry: the number of packets matching each entry, and the elapsed time since a packet last matched each entry
Configurable	True

ipv4-filter name *string*

Context	acl ipv4-filter name <i>string</i>
Tree	ipv4-filter
Description	List of IPv4 filter policies
Configurable	True

name *string*

Context	acl ipv4-filter name <i>string</i>
Description	Name of the IPv4 filter policy.
String Length	1 to 255
Configurable	True

description *string*

Context	acl ipv4-filter name <i>string</i> description <i>string</i>
Tree	description
Description	Description string for the IPv4 filter policy
String Length	1 to 255
Configurable	True

entry **sequence-id** *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Range	1 to 65535
Configurable	True

action

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> action
Tree	action
Description	Container for the actions to be applied to packets matching the filter entry.
Configurable	True

accept

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> action accept
Tree	accept
Description	Accept matching packets and forward them towards their normal destination
Configurable	True

log *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> action accept log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: <ul style="list-style-type: none">• timestamp• filter name• filter entry sequence-id• incoming interface• action: accept• IP protocol• packet-length• source-IP• source-port (TCP/UDP packets)• dest-IP• dest-port (TCP/UDP packets)• icmp-type (ICMP packets)• icmp-code (ICMP packets)
Default	false
Configurable	True

drop

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> action drop
Tree	drop
Description	Drop matching packets without sending any ICMP messages back to the source
Configurable	True

log *boolean*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> action drop log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry

The log entry contains the following information:

- timestamp
- filter name
- filter entry sequence-id
- incoming interface
- action: drop
- IP protocol
- packet-length
- source-IP
- source-port (TCP/UDP packets)
- dest-IP
- dest-port (TCP/UDP packets)
- icmp-type (ICMP packets)
- icmp-code (ICMP packets)

This action combination is not supported on Trident3 platforms when the filter is applied as an output (egress traffic) filter; no logs will be generated.

Default	false
Configurable	True

description *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> description <i>string</i>
Tree	description
Description	Description string for the filter entry
String Length	1 to 255
Configurable	True

match

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match
Tree	match
Description	Container for the conditions that determine whether a packet matches this entry
Configurable	True

destination-address *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-address <i>string</i>
Tree	destination-address
Description	A packet matches this condition if its destination IP address is within the specified IPv4 prefix.
Configurable	True

destination-port

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port
Tree	destination-port
Description	A packet matches this condition if its destination TCP or UDP port number matches the value or range that is specified The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
Configurable	True

operator *keyword*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port operator <i>keyword</i>
Tree	operator
Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- `systat`
Active Users (`systat` service)
- `tacacs`
TACACS Login Host protocol
- `talk`
Talk
- `tcpmux`
TCP Port Service Multiplexer (TCPMUX)
- `tcpnethasprv`
`tcpnethasprv`, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context **acl** **ipv4-filter name** *string* **entry sequence-id** *number* **match destination-port range start**
(*number | keyword*)

Tree **start**

Description The starting port number to include in the range

Range 0 to 65535

Options

- `acap`
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
 - Remote Procedure Call
 - daytime
 - Daytime Protocol
 - dhcpv6-client
 - DHCPv6 Client
 - dhcpv6-server
 - DHCPv6 Server
 - dhcp-failover
 - DHCP Failover Protocol
 - dicom
 - Digital Imaging and Communications in Medicine
 - discard
 - Discard Protocol. Also Wake-on-LAN.
 - dnsix
 - DNSIX security protocol auditing
 - domain
 - Domain Name System
 - dsp
 - Display Support Protocol
 - echo
 - Echo Protocol
 - epp
 - Extensible Provisioning Protocol
 - esro
 - Efficient Short Remote Operations (ESRO)
 - exec
 - Remote Process Execution (Rexec)
 - finger
 - Finger protocol
 - ftp
 - File Transfer Protocol control
 - ftp-data
 - File Transfer Protocol data
 - ftps
 - FTPS (FTP over SSL/TLS) control
 - ftps-data
 - FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetnetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match destination-port value**
(*number | keyword*)

Tree **value**

Description A destination port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

first-fragment *boolean*

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match first-fragment** *boolean*

Tree **first-fragment**

Description Match the first fragment of an IPv4 datagram

A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and and the more-fragments bit is 1. It is not valid to configure this leaf without configuring a match value for the fragment leaf.

Configurable True

fragment *boolean*

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match fragment** *boolean*

Tree **fragment**

Description Match an IPv4 fragment

A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and and the more-fragments bit is 1 or if the IPv4 header indicates that the fragment-offset is greater than 0. A packet matches the false condition if it is unfragmented.

Configurable True

icmp

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match icmp
Tree	icmp
Description	A packet matches this condition if its ICMP type and code matches one of the specified combinations The rule should also have a condition that the IP protocol equals 1 (ICMP) in order for this to be interpreted correctly.
Configurable	True

code *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match icmp code <i>number</i>
Tree	code
Description	Match if the ICMP code value is any value in the list Requires ICMP type to be specified because codes are type dependent.
Configurable	True

type (*number* | *keyword*)

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match icmp type (<i>number</i> <i>keyword</i>)
Tree	type
Description	Match a single ICMP type value.
Range	0 to 255
Options	<ul style="list-style-type: none">• echo-reply ICMP Echo Reply• dest-unreachable ICMP Destination Unreachable• source-quench ICMP Source Quench• redirect ICMP Redirect• echo ICMP Echo• router-advertise ICMP Router Advertisement• router-solicit ICMP Router Solicitation• time-exceeded

	ICMP Time Exceeded
	• param-problem
	ICMP Parameter Problem
	• timestamp
	ICMP Timestamp
	• timestamp-reply
	ICMP Timestamp Reply
Configurable	True

protocol (*number | keyword*)

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match protocol (<i>number keyword</i>)
Tree	protocol
Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Range	0 to 255
Options	<ul style="list-style-type: none">• ipv6-hop IPv6 hop-by-hop option• icmp Internet Control Message Protocol• igmp Internet Group Management Protocol• ggp Gateway-to-Gateway Protocol• ipv4 IPv4 encapsulation• st Stream Protocol• tcp Transmission Control Protocol• egp Exterior Gateway Protocol• igp Interior Gateway Protocol• udp User Datagram Protocol• ipv6 IPv6 encapsulation• idrp Inter-Domain Routing Protocol

- rsvp
Resource Reservation Protocol
- gre
Generic Routing Encapsulation
- esp
IPSec Encapsulating Security Payload
- ah
IPSec Authentication Header
- icmp6
IPSec Authentication Header
- no-next-hdr
No Next Header for IPv6
- ipv6-dest-opts
Destination Options for IPv6
- eigrp
Cisco EIGRP
- pim
Protocol Independent Multicast
- vrrp
Virtual Router Redundancy Protocol
- l2tp
Layer Two Tunneling Protocol
- sctp
Stream Control Transmission Protocol
- mpls-in-ip
MPLS Encapsulation inside IP
- rohc
Robust Header Compression

Configurable True

source-address *string*

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match source-address** *string*

Tree **source-address**

Description A packet matches this condition if its source IP address is within the specified IPv4 prefix

Configurable True

source-port

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match source-port
Tree	source-port
Description	<p>A packet matches this condition if its source TCP or UDP port number matches the value or range that is specified</p> <p>The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.</p>
Configurable	True

operator *keyword*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match source-port operator <i>keyword</i>
Tree	operator
Description	<p>Comparison operator</p> <p>eq = equal ge = greater than or equal to le = less than or equal to</p>
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match source-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number | keyword*)

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match source-port range end (<i>number keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- `systat`
Active Users (`systat` service)
- `tacacs`
TACACS Login Host protocol
- `talk`
Talk
- `tcpmux`
TCP Port Service Multiplexer (TCPMUX)
- `tcpnethasprv`
`tcpnethasprv`, Aladdin Knowledge Systems Hasp services
- `tftp`
Trivial File Transfer Protocol (TFTP)
- `time`
Time Protocol
- `timed`
Timeserver
- `ups`
Uninterruptible power supply (UPS)
- `xdmcp`
X Display Manager Control Protocol (XDMCP)
- `xns-ch`
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- `xns-mail`
Xerox Network Systems (XNS) Mail
- `xns-time`
Xerox Network Systems (XNS) Time Protocol
- `z3950`
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match source-port range start**
(*number | keyword*)

Tree **start**

Description The starting port number to include in the range

Range 0 to 65535

Options

- `acap`
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
 - Remote Procedure Call
 - daytime
 - Daytime Protocol
 - dhcpv6-client
 - DHCPv6 Client
 - dhcpv6-server
 - DHCPv6 Server
 - dhcp-failover
 - DHCP Failover Protocol
 - dicom
 - Digital Imaging and Communications in Medicine
 - discard
 - Discard Protocol. Also Wake-on-LAN.
 - dnsix
 - DNSIX security protocol auditing
 - domain
 - Domain Name System
 - dsp
 - Display Support Protocol
 - echo
 - Echo Protocol
 - epp
 - Extensible Provisioning Protocol
 - esro
 - Efficient Short Remote Operations (ESRO)
 - exec
 - Remote Process Execution (Rexec)
 - finger
 - Finger protocol
 - ftp
 - File Transfer Protocol control
 - ftp-data
 - File Transfer Protocol data
 - ftps
 - FTPS (FTP over SSL/TLS) control
 - ftps-data
 - FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match source-port value** (*number | keyword*)

Tree **value**

Description A source port number

Range 0 to 65535

- Options
- acap
Application Configuration Access Protocol
 - afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration

-
- atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server

-
- DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol

-
- gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat

-
- IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link

-
- microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews

-
- Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol

-
- qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw

-
- IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver

- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

tcp-flags *string*

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **match tcp-flags** *string*

Tree **tcp-flags**

Description A logical expression using the &, | and ! logical operators and the TCP flag names: rst, syn and ack.

Configurable True

statistics

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **statistics**

Tree **statistics**

Description Container for per-entry statistics

Configurable False

aggregate

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **statistics aggregate**

Tree **aggregate**

Description Container for aggregated per-entry statistics. Not present if the entry is part of a filter with statistics-per-entry set to false.

Configurable False

in-last-match *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate in-last-match <i>string</i>
Tree	in-last-match
Description	The elapsed time since an ingress packet last matched the entry, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an input ACL
Configurable	False

in-matched-packets *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate in-matched-packets <i>number</i>
Tree	in-matched-packets
Description	The number of ingress packets matching the entry since it was programmed or since the last clear, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an input ACL
Default	0
Configurable	False

out-last-match *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate out-last-match <i>string</i>
Tree	out-last-match
Description	The elapsed time since an egress packet last matched the entry, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an output ACL
Configurable	False

out-matched-packets *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate out-matched-packets <i>number</i>
Tree	out-matched-packets
Description	The number of egress packets matching the entry since it was programmed or since the last clear, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an output ACL
Default	0
Configurable	False

last-clear *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level or a higher level
Configurable	False

per-interface

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Description	Container for per-entry statistics on a per interface basis. Not present if the entry is part of a filter with statistics-per-entry set to false.
Configurable	False

subinterface name *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Description	If subinterface-specific=disabled then this list is empty. If subinterface-specific=input-only then this is the list of subinterfaces that apply the ACL as an input ACL If subinterface-specific=output-only then this is the list of subinterfaces that apply the ACL as an output ACL. If subinterface-specific=input-and-output then this is the list of subinterfaces that apply the ACL as an input ACL or an output ACL.
Configurable	False

name *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Description	Reference to a subinterface.
Configurable	False

in-last-match *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> in-last-match <i>string</i>
Tree	in-last-match
Description	The elapsed time since an ingress packet last matched the entry on this specific subinterface. Updated only if subinterface-specific is set to input-only or input-and-output
Configurable	False

in-matched-packets *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> in-matched-packets <i>number</i>
Tree	in-matched-packets
Description	The number of ingress packets matching the entry on this specific subinterface. Incremented only if subinterface-specific is set to input-only or input-and-output
Default	0
Configurable	False

last-clear *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level or a higher level
Configurable	False

out-last-match *string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> out-last-match <i>string</i>
Tree	out-last-match
Description	The elapsed time since an egress packet last matched the entry on this specific subinterface. Updated only if subinterface-specific is set to output-only or input-and-output
Configurable	False

out-matched-packets *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> out-matched-packets <i>number</i>
Tree	out-matched-packets
Description	The number of egress packets matching the entry on this specific subinterface. Incremented only if subinterface-specific is set to output-only or input-and-output
Default	0
Configurable	False

tcam-entries

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries
Tree	tcam-entries
Description	Information about the TCAM entries used to implement the ACL entry
Configurable	False

linecard slot *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i>
Tree	linecard
Description	List of linecards in the system
Configurable	False

slot *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i>
Description	Slot identifier
Range	1 to 10
Configurable	False

input-total *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i> input-total <i>number</i>
Tree	input-total
Description	The number of TCAM entries required to implement this entry on all subinterfaces of this slot where the filter is applied to ingress traffic.

For example, if a single-instance of the entry takes 2 TCAM entries and the filter is an output-only subinterface-specific filter and the filter is applied to 5 subinterfaces on output and to 5 subinterfaces on input then input-total=2. If the entry is not applied to ingress traffic on any subinterfaces of this slot then input-total=0.

Configurable False

output-total *number*

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **tcam-entries linecard slot** *number*
output-total *number*

Tree **output-total**

Description The number of TCAM entries required to implement this entry on all subinterfaces of this slot where the filter is applied to egress traffic.

For example, if a single-instance of the entry takes 2 TCAM entries and the filter is an output-only subinterface-specific filter and the filter is applied to 5 subinterfaces on output and to 5 subinterfaces on input then output-total=10. If the entry is not applied to egress traffic on any subinterfaces of this slot then output-total=0.

Configurable False

single-instance *number*

Context **acl ipv4-filter name** *string* **entry sequence-id** *number* **tcam-entries linecard slot** *number*
single-instance *number*

Tree **single-instance**

Description The number of TCAM entries required to implement this entry if it is applied to only one subinterface and one traffic direction specific to this slot.

This is non-zero even if the filter is not applied to any subinterfaces of this slot. It captures the effect of TCAM entry expansion to deal with port ranges, for example.

Configurable False

last-clear *string*

Context **acl ipv4-filter name** *string* **last-clear** *string*

Tree **last-clear**

Description Time of the last clear command performed by the user at this level

Configurable False

statistics

Context	acl ipv4-filter name <i>string</i> statistics
Tree	statistics
Description	Statistics container
Configurable	False

statistics-per-entry *boolean*

Context	acl ipv4-filter name <i>string</i> statistics-per-entry <i>boolean</i>
Tree	statistics-per-entry
Description	Collect statistics for each entry of the ACL The exact set of statistics depend on the subinterface-specific mode
Configurable	True

subinterface-specific *keyword*

Context	acl ipv4-filter name <i>string</i> subinterface-specific <i>keyword</i>
Tree	subinterface-specific
Description	Controls the instantiation of the filter when it is applied as an input or output ACL disabled: all subinterfaces on a single linecard that reference the ACL as an input ACL use a shared filter instance, and all subinterfaces on a single linecard that reference the ACL as an output ACL use a shared filter instance input-only: all subinterfaces on a single linecard that reference the ACL as an output ACL use a shared filter instance, but each subinterface that references the ACL as an input ACL uses its own separate instance of the filter output-only: all subinterfaces on a single linecard that reference the ACL as an input ACL use a shared filter instance, but each subinterface that references the ACL as an output ACL uses its own separate instance of the filter input-and-output: each subinterface that references the ACL as either an input ACL or an output ACL uses its own separate instance of the filter
Default	disabled
Options	<ul style="list-style-type: none">• disabled• input-only• output-only• input-and-output
Configurable	True

ipv6-filter name *string*

Context	acl ipv6-filter name <i>string</i>
Tree	ipv6-filter
Description	List of IPv6 filter policies
Configurable	True

name *string*

Context	acl ipv6-filter name <i>string</i>
Description	Name of the IPv6 filter policy.
String Length	1 to 255
Configurable	True

description *string*

Context	acl ipv6-filter name <i>string</i> description <i>string</i>
Tree	description
Description	Description string for the IPv6 filter policy
String Length	1 to 255
Configurable	True

entry sequence-id *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries.
Range	1 to 65535
Configurable	True

action

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> action
Tree	action
Description	Container for the actions to be applied to packets matching the filter entry.
Configurable	True

accept

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> action accept
Tree	accept
Description	Accept matching packets and forward them towards their normal destination
Configurable	True

log *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> action accept log <i>boolean</i>
---------	--

Tree **log**

Description When this is true, a log is created for each packet matching the entry

The log entry contains the following information:

- timestamp
- filter name
- filter entry sequence-id
- incoming interface
- action: accept
- IP protocol
- packet-length
- source-IP
- source-port (TCP/UDP packets)
- dest-IP
- dest-port (TCP/UDP packets)
- icmp-type (ICMP packets)

	<ul style="list-style-type: none">icmp-code (ICMP packets)
Default	false
Configurable	True

drop

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> action drop
Tree	drop
Description	Drop matching packets without sending any ICMP messages back to the source
Configurable	True

log *boolean*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> action drop log <i>boolean</i>
Tree	log
Description	When this is true, a log is created for each packet matching the entry

The log entry contains the following information:

- timestamp
- filter name
- filter entry sequence-id
- incoming interface
- action: drop
- IP protocol
- packet-length
- source-IP
- source-port (TCP/UDP packets)
- dest-IP
- dest-port (TCP/UDP packets)
- icmp-type (ICMP packets)
- icmp-code (ICMP packets)

This action combination is not supported on Trident3 platforms when the filter is applied as an output (egress traffic) filter; no logs will be generated.

Default	false
Configurable	True

description *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> description <i>string</i>
Tree	description
Description	Description string for the filter entry
String Length	1 to 255
Configurable	True

match

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match
Tree	match
Description	Container for the conditions that determine whether a packet matches this entry
Configurable	True

destination-address *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-address <i>string</i>
Tree	destination-address
Description	A packet matches this condition if its destination IP address is within the specified IPv6 prefix
Configurable	True

destination-port

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port
Tree	destination-port
Description	A packet matches this condition if its destination TCP or UDP port number matches the value or range that is specified The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
Configurable	True

operator *keyword*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port operator <i>keyword</i>
Tree	operator
Description	Comparison operator

	eq = equal ge = greater than or equal to le = less than or equal to
Options	<ul style="list-style-type: none">• le Less than or equal.• ge Greater than or equal.• eq Equal to.
Configurable	True

range

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number* | *keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth

-
- Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine

-
- discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname

-
- NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol

-
- kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor

-
- Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who

-
- nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct

-
- RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps

-
- snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch

	Xerox Network Systems (XNS) Clearinghouse (Name Server)
	• xns-mail Xerox Network Systems (XNS) Mail
	• xns-time Xerox Network Systems (XNS) Time Protocol
	• z3950 ANSI Z39.50
Configurable	True

start (*number | keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port range start (<i>number keyword</i>)
Tree	start
Description	The starting port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp

-
- Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol

-
- echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt

-
- http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password

-
- kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp

-
- Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)

-
- odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip

-
- Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service

-
- ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
 - xns-mail
Xerox Network Systems (XNS) Mail
 - xns-time
Xerox Network Systems (XNS) Time Protocol
 - z3950
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port value (<i>number keyword</i>)
Tree	value
Description	A destination port number
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- **systat**
Active Users (systat service)
- **tacacs**
TACACS Login Host protocol
- **talk**
Talk
- **tcpmux**
TCP Port Service Multiplexer (TCPMUX)
- **tcpnethasprv**
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- **tftp**
Trivial File Transfer Protocol (TFTP)
- **time**
Time Protocol
- **timed**
Timeserver
- **ups**
Uninterruptible power supply (UPS)
- **xdmcp**
X Display Manager Control Protocol (XDMCP)
- **xns-ch**
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- **xns-mail**
Xerox Network Systems (XNS) Mail
- **xns-time**
Xerox Network Systems (XNS) Time Protocol
- **z3950**
ANSI Z39.50

Configurable True

icmp6

Context **acl ipv6-filter name string entry sequence-id number match icmp6**

Tree **icmp6**

Description A packet matches this condition if its ICMPv6 type and code matches one of the specified combinations

The rule should also have a condition that the next-header value equals 58 (ICMPv6) in order for this to be interpreted correctly.

Configurable True

code *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match icmp6 code <i>number</i>
Tree	code
Description	Match if the ICMPv6 code value is any value in the list Requires ICMPv6 type to be specified because codes are type dependent.
Configurable	True

type (*number | keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match icmp6 type (<i>number keyword</i>)
Tree	type
Description	Match a single ICMPv6 type value
Range	0 to 255
Options	<ul style="list-style-type: none">• dest-unreachable ICMPv6 Destination Unreachable• packet-too-big ICMPv6 Packet Too Big• time-exceeded ICMPv6 Time Exceeded• param-problem Parameter Problem• echo-request ICMPv6 Echo Request• echo-reply ICMPv6 Echo Reply• mld-query Multicast Listener Discovery Query• mld-report Multicast Listener Discovery Report• mld-done Multicast Listener Discovery Done• router-solicit ICMPv6 Router Solicitation• router-advertise ICMPv6 Router Advertisement• neighbor-solicit ICMPv6 Neighbor Solicitation

- neighbor-advertise
ICMPv6 Neighbor Advertisement
- redirect
ICMPv6 Redirect
- router-renumber
ICMPv6 Router Renumbering
- node-info-query
ICMPv6 Node Information Query
- node-info-response
ICMPv6 Node Information Response
- mld-v2
Multicast Listener Discovery Version 2
- mcast-rtr-adv
Multicast Router Advertisement
- mcast-rtr-solicit
Multicast Router Solicitation
- mcast-rtr-term
Multicast Router Termination

Configurable True

next-header (*number | keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match next-header (<i>number keyword</i>)
Tree	next-header
Description	An IPv6 packet matches this condition if its first next-header field (in the IPv6 fixed header) contains the specified value
Range	0 to 255
Options	<ul style="list-style-type: none">• ipv6-hop IPv6 hop-by-hop option• icmp Internet Control Message Protocol• igmp Internet Group Management Protocol• ggp Gateway-to-Gateway Protocol• ipv4 IPv4 encapsulation• st

-
- Stream Protocol
 - tcp
Transmission Control Protocol
 - egp
Exterior Gateway Protocol
 - igp
Interior Gateway Protocol
 - udp
User Datagram Protocol
 - ipv6
IPv6 encapsulation
 - idrp
Inter-Domain Routing Protocol
 - rsvp
Resource Reservation Protocol
 - gre
Generic Routing Encapsulation
 - esp
IPSec Encapsulating Security Payload
 - ah
IPSec Authentication Header
 - icmp6
IPSec Authentication Header
 - no-next-hdr
No Next Header for IPv6
 - ipv6-dest-opts
Destination Options for IPv6
 - eigrp
Cisco EIGRP
 - pim
Protocol Independent Multicast
 - vrrp
Virtual Router Redundancy Protocol
 - l2tp
Layer Two Tunneling Protocol
 - sctp
Stream Control Transmission Protocol
 - mpls-in-ip
MPLS Encapsulation inside IP

- rohc
Robust Header Compression
- Configurable True

source-address *string*

- Context **acl ipv6-filter name** *string* **entry sequence-id** *number* **match source-address** *string*
- Tree **source-address**
- Description A packet matches this condition if its source IP address is within the specified IPv6 prefix
- Configurable True

source-port

- Context **acl ipv6-filter name** *string* **entry sequence-id** *number* **match source-port**
- Tree **source-port**
- Description A packet matches this condition if its source TCP or UDP port number matches the value or range that is specified
- The rule should also have a condition that the IP protocol equals 6 (TCP) or 17 (UDP) in order for this to be interpreted correctly.
- Configurable True

operator *keyword*

- Context **acl ipv6-filter name** *string* **entry sequence-id** *number* **match source-port operator** *keyword*
- Tree **operator**
- Description Comparison operator
- eq = equal ge = greater than or equal to le = less than or equal to
- Options
- le
Less than or equal.
 - ge
Greater than or equal.
 - eq
Equal to.
- Configurable True

range

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-port range
Tree	range
Description	Container used to specify a contiguous range of TCP/UDP port numbers
Configurable	True

end (*number* | *keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
Description	The ending port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp

-
- Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol

-
- epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc

-
- Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell

-
- l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange

-
- MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)

-
- olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje

-
- Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol

-
- submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)
 - tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
 - tftp
Trivial File Transfer Protocol (TFTP)
 - time
Time Protocol
 - timed
Timeserver
 - ups
Uninterruptible power supply (UPS)
 - xdmcp
X Display Manager Control Protocol (XDMCP)
 - xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
 - xns-mail
Xerox Network Systems (XNS) Mail
 - xns-time
Xerox Network Systems (XNS) Time Protocol
 - z3950
ANSI Z39.50

Configurable True

start (*number | keyword*)

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-port range start (<i>number keyword</i>)
Tree	start
Description	The starting port number to include in the range
Range	0 to 65535
Options	<ul style="list-style-type: none">• acap Application Configuration Access Protocol• afp-tcp Apple Filing Protocol over TCP• arns A Remote Network Server System• asf-rmcp ASF Remote Management and Control Protocol & IPMI Remote Management Protocol• ashare AppleShare IP Web Administration• atalk-rm AppleTalk Routing Maintenance• aurp AppleTalk Update-Based Routing Protocol• auth Authentication Service• bfd Bidirectional Forwarding Detection Single Hop• bfd-echo BFD Echo• bftp Background File Transfer Program• bgmp Border Gateway Multicast Protocol• bgp Border Gateway Protocol• bootpc Bootstrap Protocol (BOOTP) Client and DHCP Client• bootps Bootstrap Protocol (BOOTP) Server and DHCP Server• ccso-ns CCSO Nameserver• chargen

-
- Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce
Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol

-
- ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data
 - godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3

-
- Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx
Internetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol

-
- Imp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo
 - mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp

-
- NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4
NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)

-
- pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)
 - ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor

-
- rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp
Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)

- **systat**
Active Users (systat service)
- **tacacs**
TACACS Login Host protocol
- **talk**
Talk
- **tcpmux**
TCP Port Service Multiplexer (TCPMUX)
- **tcpnethasprv**
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- **tftp**
Trivial File Transfer Protocol (TFTP)
- **time**
Time Protocol
- **timed**
Timeserver
- **ups**
Uninterruptible power supply (UPS)
- **xdmcp**
X Display Manager Control Protocol (XDMCP)
- **xns-ch**
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- **xns-mail**
Xerox Network Systems (XNS) Mail
- **xns-time**
Xerox Network Systems (XNS) Time Protocol
- **z3950**
ANSI Z39.50

Configurable True

value (*number | keyword*)

Context **acl ipv6-filter name** *string* **entry sequence-id** *number* **match source-port value** (*number | keyword*)

Tree **value**

Description A source port number

Range 0 to 65535

Options

- **acap**
Application Configuration Access Protocol

-
- afp-tcp
Apple Filing Protocol over TCP
 - arns
A Remote Network Server System
 - asf-rmcp
ASF Remote Management and Control Protocol & IPMI Remote Management Protocol
 - ashare
AppleShare IP Web Administration
 - atalk-rm
AppleTalk Routing Maintenance
 - aurp
AppleTalk Update-Based Routing Protocol
 - auth
Authentication Service
 - bfd
Bidirectional Forwarding Detection Single Hop
 - bfd-echo
BFD Echo
 - bftp
Background File Transfer Program
 - bgmp
Border Gateway Multicast Protocol
 - bgp
Border Gateway Protocol
 - bootpc
Bootstrap Protocol (BOOTP) Client and DHCP Client
 - bootps
Bootstrap Protocol (BOOTP) Server and DHCP Server
 - ccso-ns
CCSO Nameserver
 - chargen
Character Generator Protocol (CHARGEN)
 - cisco-tdp
Cisco Tag Distribution Protocol
 - citadel
Citadel
 - clearcase
ClearCase albd
 - commerce

-
- Commerce Applications
 - courier
Remote Procedure Call
 - daytime
Daytime Protocol
 - dhcpv6-client
DHCPv6 Client
 - dhcpv6-server
DHCPv6 Server
 - dhcp-failover
DHCP Failover Protocol
 - dicom
Digital Imaging and Communications in Medicine
 - discard
Discard Protocol. Also Wake-on-LAN.
 - dnsix
DNSIX security protocol auditing
 - domain
Domain Name System
 - dsp
Display Support Protocol
 - echo
Echo Protocol
 - epp
Extensible Provisioning Protocol
 - esro
Efficient Short Remote Operations (ESRO)
 - exec
Remote Process Execution (Rexec)
 - finger
Finger protocol
 - ftp
File Transfer Protocol control
 - ftp-data
File Transfer Protocol data
 - ftps
FTPS (FTP over SSL/TLS) control
 - ftps-data
FTPS (FTP over SSL/TLS) data

-
- godi
Group Domain Of Interpretation (GDOI) protocol
 - gopher
Gopher protocol
 - gtp-c
GTP control messages (GTP-C)
 - gtp-prime
GTP prime CDR logging protocol
 - gtp-u
GTP user data messages (GTP-U)
 - ha-cluster
Linux-HA high-availability heartbeat
 - hostname
NIC hostname server
 - hp-alarm-mgr
HP data alarm manager
 - http
Hypertext Transfer Protocol
 - http-alt
FileMaker Web Sharing (HTTP Alternate)
 - http-mgmt
http-mgmt
 - http-rpc
Remote procedure call over Hypertext Transfer Protocol
 - https
Hypertext Transfer Protocol over TLS/SSL
 - ieee-mms-ssl
IEEE Media Management System over SSL
 - imap
Internet Message Access Protocol (IMAP)
 - imap3
Internet Message Access Protocol (IMAP), version 3
 - imaps
Internet Message Access Protocol over TLS/SSL
 - ipp
Internet Printing Protocol
 - ipsec
Internet Protocol Security (IPSec)
 - ipx

-
- Internetnetwork Packet Exchange (IPX)
 - irc
Internet Relay Chat (IRC)
 - iris-beep
IRIS (Internet Registry Information Service) over BEEP
 - isakmp
Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
 - isakmp-nat
IPSec NAT Traversal
 - iscsi
iSCSI
 - iso-tsap
ISO Transport Service Access Point (TSAP) Class 0 protocol
 - kerberos
Kerberos authentication system
 - kerberos-adm
Kerberos administration
 - klogin
Kerberos login
 - kpasswd
Kerberos Change/Set password
 - kshell
Kerberos Remote shell
 - l2tp
Layer 2 Forwarding Protocol (L2F) and Layer 2 Tunneling Protocol (L2TP)
 - ldap
Lightweight Directory Access Protocol (LDAP)
 - ldaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
 - ldp
Label Distribution Protocol
 - lmp
Link Management Protocol (LMP)
 - login
rlogin (TCP) or Who (UDP)
 - lpd
Line Printer Daemon
 - lsp-ping
MPLS LSP-echo

-
- mac-server-adm
Mac OS X Server administration
 - matip-a
Mapping of Airline Traffic over Internet Protocol (MATIP) type A
 - matip-b
Mapping of Airline Traffic over Internet Protocol (MATIP) type B
 - micro-bfd
BFD session over each LAG member link
 - microsoft-ds
Microsoft Directory Services
 - mobile-ip
Mobile IP Agent
 - monitor
Monitor
 - mpp
Message posting protocol (MPP)
 - mssql-m
Microsoft SQL Server database management system (MSSQL) monitor
 - mssql-s
Microsoft SQL Server database management system (MSSQL) server
 - msdp
Multicast Source Discovery Protocol
 - ms-exchange
MS Exchange Routing
 - msp
Message Send Protocol
 - multihop-bfd
Bidirectional Forwarding Detection Multi-Hop
 - nas
Netnews Administration System (NAS)
 - ncp
NetWare Core Protocol
 - netrjs-1
NETRJS protocol
 - netrjs-2
NETRJS protocol
 - netrjs-3
NETRJS protocol
 - netrjs-4

-
- NETRJS protocol
 - netbios-data
NetBIOS Datagram Service
 - netbios-ns
NetBIOS Name Service
 - netbios-ss
NetBIOS Session Service
 - netnews
Netnews
 - netwall
netwall, for Emergency Broadcasts
 - new-rwho
new-rwho, new-who
 - nfs
Network File System (NFS)
 - nntp
Network News Transfer Protocol (NNTP)
 - nntps
Network News Transfer Protocol over TLS/SSL (NNTPS)
 - ntp
Network Time Protocol (NTP)
 - odmr
On-Demand Mail Relay (ODMR)
 - olsr
Optimized Link State Routing (OLSR)
 - openvpn
OpenVPN
 - pim-auto-rp
PIM Auto-RP
 - pkix-timestamp
PKIX Time Stamp Protocol (TSP)
 - pop2
Post Office Protocol, version 2 (POP2)
 - pop3
Post Office Protocol, version 3 (POP3)
 - pop3s
Post Office Protocol 3 over TLS/SSL (POP3S)
 - pptp
Point-to-Point Tunneling Protocol (PPTP)

-
- ptp-event
Precision Time Protocol (PTP) event messages
 - ptp-general
Precision Time Protocol (PTP) general messages
 - print-srv
Network PostScript print server
 - qmtp
Quick Mail Transfer Protocol
 - qotd
Quote of the Day (QOTD)
 - radius
RADIUS authentication protocol
 - radius-acct
RADIUS accounting protocol
 - remote-mail
Remote Mail Checking Protocol
 - remotefs
Remotefs, RFS Server
 - remotecmd
SupportSoft Nexus Remote Command
 - rip
Routing Information Protocol
 - rje
Remote Job Entry
 - rlp
Resource Location Protocol
 - rlzdb
RLZ DBase
 - rmc
IBM RMC (Remote monitoring and Control) protocol
 - rmonitor
rmonitor, Remote Monitor
 - rpc2portmap
Rpc2portmap
 - rsync
rsync file synchronization protocol
 - rtelnet
Remote User Telnet Service (RTelnet)
 - rtsp

-
- Real Time Streaming Protocol (RTSP)
 - sgmp
Simple Gateway Monitoring Protocol (SGMP)
 - silc
Secure Internet Live Conferencing (SILC)
 - smux
SNMP multiplexing protocol (SMUX)
 - sna-gw
IBM Systems Network Architecture (SNA) gateway access server
 - snmp
Simple Network Management Protocol (SNMP)
 - snmp-trap
SNMP Traps
 - snpp
Simple Network Paging Protocol (SNPP)
 - smtp
Simple Mail Transfer Protocol (SMTP)
 - sql-svcs
Structured Query Language (SQL) Services
 - sql
Structured Query Language (SQL) Service
 - ssh
Secure Shell Protocol
 - submission
Email message submission (SMTP)
 - sunrpc
Open Network Computing Remote Procedure Call (ONC RPC), also Sun RPC
 - svcloc
Service Location Protocol (SLP)
 - syslog
Syslog (UDP) and Remote Shell (TCP)
 - systat
Active Users (systat service)
 - tacacs
TACACS Login Host protocol
 - talk
Talk
 - tcpmux
TCP Port Service Multiplexer (TCPMUX)

- tcpnethasprv
tcpnethasprv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups
Uninterruptible power supply (UPS)
- xdmcp
X Display Manager Control Protocol (XDMCP)
- xns-ch
Xerox Network Systems (XNS) Clearinghouse (Name Server)
- xns-mail
Xerox Network Systems (XNS) Mail
- xns-time
Xerox Network Systems (XNS) Time Protocol
- z3950
ANSI Z39.50

Configurable True

tcp-flags *string*

Context **acl ipv6-filter name** *string* **entry sequence-id** *number* **match tcp-flags** *string*

Tree **tcp-flags**

Description A logical expression using the &, | and ! logical operators and the TCP flag names: rst, syn and ack.

Configurable True

statistics

Context **acl ipv6-filter name** *string* **entry sequence-id** *number* **statistics**

Tree **statistics**

Description Container for per-entry statistics

Configurable False

aggregate

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate
Tree	aggregate
Description	Container for aggregated per-entry statistics. Not present if the entry is part of a filter with statistics-per-entry set to false.
Configurable	False

in-last-match *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate in-last-match <i>string</i>
Tree	in-last-match
Description	The elapsed time since an ingress packet last matched the entry, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an input ACL
Configurable	False

in-matched-packets *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate in-matched-packets <i>number</i>
Tree	in-matched-packets
Description	The number of ingress packets matching the entry since it was programmed or since the last clear, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an input ACL
Default	0
Configurable	False

out-last-match *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate out-last-match <i>string</i>
Tree	out-last-match
Description	The elapsed time since an egress packet last matched the entry, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an output ACL
Configurable	False

out-matched-packets *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate out-matched-packets <i>number</i>
Tree	out-matched-packets
Description	The number of egress packets matching the entry since it was programmed or since the last clear, considering the mgmt0 subinterface and all subinterfaces of all linecard ports that use the ACL as an output ACL
Default	0
Configurable	False

last-clear *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level or a higher level
Configurable	False

per-interface

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Description	Container for per-entry statistics on a per interface basis. Not present if the entry is part of a filter with statistics-per-entry set to false.
Configurable	False

subinterface name *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Description	If subinterface-specific=disabled then this list is empty. If subinterface-specific=input-only then this is the list of subinterfaces that apply the ACL as an input ACL If subinterface-specific=output-only then this is the list of subinterfaces that apply the ACL as an output ACL. If subinterface-specific=input-and-output then this is the list of subinterfaces that apply the ACL as an input ACL or an output ACL.
Configurable	False

name *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Description	Reference to a subinterface.
Configurable	False

in-last-match *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> in-last-match <i>string</i>
Tree	in-last-match
Description	The elapsed time since an ingress packet last matched the entry on this specific subinterface. Updated only if subinterface-specific is set to input-only or input-and-output
Configurable	False

in-matched-packets *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> in-matched-packets <i>number</i>
Tree	in-matched-packets
Description	The number of ingress packets matching the entry on this specific subinterface. Incremented only if subinterface-specific is set to input-only or input-and-output
Default	0
Configurable	False

last-clear *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level or a higher level
Configurable	False

out-last-match *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> out-last-match <i>string</i>
Tree	out-last-match
Description	The elapsed time since an egress packet last matched the entry on this specific subinterface. Updated only if subinterface-specific is set to output-only or input-and-output
Configurable	False

out-matched-packets *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> out-matched-packets <i>number</i>
Tree	out-matched-packets
Description	The number of egress packets matching the entry on this specific subinterface. Incremented only if subinterface-specific is set to output-only or input-and-output
Default	0
Configurable	False

tcam-entries

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries
Tree	tcam-entries
Description	Information about the TCAM entries used to implement the ACL entry
Configurable	False

linecard slot *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i>
Tree	linecard
Description	List of linecards in the system
Configurable	False

slot *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i>
Description	Slot identifier
Range	1 to 10
Configurable	False

input-total *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i> input-total <i>number</i>
Tree	input-total
Description	<p>The number of TCAM entries required to implement this entry on all subinterfaces of this slot where the filter is applied to ingress traffic.</p> <p>For example, if a single-instance of the entry takes 2 TCAM entries and the filter is an output-only subinterface-specific filter and the filter is applied to 5 subinterfaces on output and to 5 subinterfaces on input then input-total=2. If the entry is not applied to ingress traffic on any subinterfaces of this slot then input-total=0.</p>
Configurable	False

output-total *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i> output-total <i>number</i>
Tree	output-total
Description	<p>The number of TCAM entries required to implement this entry on all subinterfaces of this slot where the filter is applied to egress traffic.</p> <p>For example, if a single-instance of the entry takes 2 TCAM entries and the filter is an output-only subinterface-specific filter and the filter is applied to 5 subinterfaces on output and to 5 subinterfaces on input then output-total=10. If the entry is not applied to egress traffic on any subinterfaces of this slot then output-total=0.</p>
Configurable	False

single-instance *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot <i>number</i> single-instance <i>number</i>
Tree	single-instance
Description	<p>The number of TCAM entries required to implement this entry if it is applied to only one subinterface and one traffic direction specific to this slot.</p> <p>This is non-zero even if the filter is not applied to any subinterfaces of this slot. It captures the effect of TCAM entry expansion to deal with port ranges, for example.</p>
Configurable	False

last-clear *string*

Context	acl ipv6-filter name <i>string</i> last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command performed by the user at this level
Configurable	False

statistics

Context	acl ipv6-filter name <i>string</i> statistics
Tree	statistics
Description	Statistics container
Configurable	False

statistics-per-entry *boolean*

Context	acl ipv6-filter name <i>string</i> statistics-per-entry <i>boolean</i>
Tree	statistics-per-entry
Description	Collect statistics for each entry of the ACL The exact set of statistics depend on the subinterface-specific mode
Configurable	True

subinterface-specific *keyword*

Context	acl ipv6-filter name <i>string</i> subinterface-specific <i>keyword</i>
Tree	subinterface-specific
Description	Controls the instantiation of the filter when it is applied as an input or output ACL disabled: all subinterfaces on a single linecard that reference the ACL as an input ACL use a shared filter instance, and all subinterfaces on a single linecard that reference the ACL as an output ACL use a shared filter instance input-only: all subinterfaces on a single linecard that reference the ACL as an output ACL use a shared filter instance, but each subinterface that references the ACL as an input ACL uses its own separate instance of the filter output-only: all subinterfaces on a single linecard that reference the ACL as an input ACL use a shared filter instance, but each subinterface that references the ACL as an output ACL uses its own separate instance of the filter

	input-and-output: each subinterface that references the ACL as either an input ACL or an output ACL uses its own separate instance of the filter
Default	disabled
Options	<ul style="list-style-type: none">• disabled• input-only• output-only• input-and-output
Configurable	True

policers

Context	acl policers
Tree	policers
Description	Container for policer definitions used by ACL entries
Configurable	True

policer name *string*

Context	acl policers policer name <i>string</i>
Tree	policer
Description	List of hardware policer templates. For each policer in this list one or more policer instances are implemented in the linecards of the system.
Configurable	True

name *string*

Context	acl policers policer name <i>string</i>
Description	User-defined name of the policer
String Length	1 to 255
Configurable	True

entry-specific *boolean*

Context	acl policers policer name <i>string</i> entry-specific <i>boolean</i>
Tree	entry-specific
Description	If set to false, only one policer instance is created from this template and it is shared by all entries of all cpm-filter ACLs that refer to this policer.

If set to true, multiple policer instances are created from this template, one for each cpm-filter entry that refers to the policer template.

Default false
Configurable True

max-burst *number*

Context **acl policers policer name** *string max-burst number*
Tree **max-burst**
Description The MBS bucket depth in bytes
Range 1 to 125000000
Units bytes
Configurable True

peak-rate *number*

Context **acl policers policer name** *string peak-rate number*
Tree **peak-rate**
Description The PIR rate in kbps (bucket empty/fill rate). This is a per J2 core, per linecard rate.
Range 1 to 1000000
Units kbps
Configurable True

statistics

Context **acl policers policer name** *string statistics*
Tree **statistics**
Description Container for linecard policer statistics
None of these statistics are populated if the policer is configured as entry-specific=true.
Configurable False

conforming-octets *number*

Context	acl policers policer name <i>string</i> statistics conforming-octets <i>number</i>
Tree	conforming-octets
Description	The number of bytes that were considered conforming by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

conforming-packets *number*

Context	acl policers policer name <i>string</i> statistics conforming-packets <i>number</i>
Tree	conforming-packets
Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Default	0
Configurable	False

exceeding-octets *number*

Context	acl policers policer name <i>string</i> statistics exceeding-octets <i>number</i>
Tree	exceeding-octets
Description	The number of bytes that were considered exceeding by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

exceeding-packets *number*

Context	acl policers policer name <i>string</i> statistics exceeding-packets <i>number</i>
Tree	exceeding-packets
Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Default	0
Configurable	False

last-clear *string*

Context	acl policers policer name <i>string</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command that applied to these statistics
Configurable	False

system-cpu-policer [name](#) *string*

Context	acl policers system-cpu-policer name <i>string</i>
Tree	system-cpu-policer
Description	List of system CPU policer templates. For each policer in this list one or more policer instances are implemented in the XDP-CPM software and these policer instances process the aggregate of terminating traffic received from all linecards.
Configurable	True

name *string*

Context	acl policers system-cpu-policer name <i>string</i>
Description	User-defined name of the policer
String Length	1 to 255
Configurable	True

entry-specific *boolean*

Context	acl policers system-cpu-policer name <i>string</i> entry-specific <i>boolean</i>
Tree	entry-specific
Description	If set to false, only one policer instance is created from this template and it is shared by all entries of all cpm-filter ACLs that refer to this policer. If set to true, multiple policer instances are created from this template, one for each cpm-filter entry that refers to the policer template.
Default	false
Configurable	True

max-packet-burst *number*

Context	acl policers system-cpu-policer name <i>string</i> max-packet-burst <i>number</i>
Tree	max-packet-burst
Description	The maximum depth of the policer bucket in number of packets
Range	16 to 4000000
Default	16
Configurable	True

peak-packet-rate *number*

Context	acl policers system-cpu-policer name <i>string</i> peak-packet-rate <i>number</i>
Tree	peak-packet-rate
Description	The maximum number of packets per second (bucket empty/fill rate)
Range	1 to 4000000
Configurable	True

statistics

Context	acl policers system-cpu-policer name <i>string</i> statistics
Tree	statistics
Description	Container for system CPU policer statistics None of these statistics are populated if the policer is configured as entry-specific=true.
Configurable	False

conforming-octets *number*

Context	acl policers system-cpu-policer name <i>string</i> statistics conforming-octets <i>number</i>
Tree	conforming-octets
Description	The number of bytes that were considered conforming by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

conforming-packets *number*

Context	acl policers system-cpu-policer name <i>string</i> statistics conforming-packets <i>number</i>
Tree	conforming-packets
Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Default	0
Configurable	False

exceeding-octets *number*

Context	acl policers system-cpu-policer name <i>string</i> statistics exceeding-octets <i>number</i>
Tree	exceeding-octets
Description	The number of bytes that were considered exceeding by the policer. The byte count includes 18 bytes of Ethernet overhead for every IP packet.
Default	0
Configurable	False

exceeding-packets *number*

Context	acl policers system-cpu-policer name <i>string</i> statistics exceeding-packets <i>number</i>
Tree	exceeding-packets
Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Default	0
Configurable	False

last-clear *string*

Context	acl policers system-cpu-policer name <i>string</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Time of the last clear command that applied to these statistics
Configurable	False

3 bfd

bfd

- + **micro-bfd-sessions**
 - + **lag-interface name** *reference*
 - + **admin-state** *keyword*
 - + **desired-minimum-transmit-interval** *number*
 - + **detection-multiplier** *number*
 - + **local-address** (*ipv4-address | ipv6-address*)
 - **member-interface name** *string*
 - **active-receive-interval** *number*
 - **active-transmit-interval** *number*
 - **async**
 - **last-clear** *string*
 - **last-packet-received** *string*
 - **last-packet-transmitted** *string*
 - **received-errored-packets** *number*
 - **received-packets** *number*
 - **transmitted-packets** *number*
 - **up-transitions** *number*
 - **failure-transitions** *number*
 - **last-failure-time** *string*
 - **last-state-transition** *string*
 - **local-diagnostic-code** *keyword*
 - **local-discriminator** *number*
 - **remote-control-plane-independent** *boolean*
 - **remote-diagnostic-code** *keyword*
 - **remote-discriminator** *number*
 - **remote-minimum-receive-interval** *number*
 - **remote-multiplier** *number*
 - **remote-session-state** *keyword*
 - **session-state** *keyword*
 - + **remote-address** (*ipv4-address | ipv6-address*)
 - + **required-minimum-receive** *number*
 - **network-instance name** *string*
 - **peer local-discriminator** *number*
 - **active-receive-interval** *number*
 - **active-transmit-interval** *number*
 - **async**
 - **last-clear** *string*
 - **last-packet-received** *string*
 - **last-packet-transmitted** *string*
 - **received-errored-packets** *number*
 - **received-packets** *number*
 - **transmitted-packets** *number*
 - **up-transitions** *number*
 - **failure-transitions** *number*
 - **last-failure-time** *string*
 - **last-state-transition** *string*
 - **local-address** (*ipv4-address | ipv6-address*)
 - **local-diagnostic-code** *keyword*
 - **oper-state** *keyword*

-
- **remote-address** (*ipv4-address | ipv6-address*)
 - **remote-control-plane-independent** *boolean*
 - **remote-diagnostic-code** *keyword*
 - **remote-discriminator** *number*
 - **remote-minimum-receive-interval** *number*
 - **remote-multiplier** *number*
 - **remote-session-state** *keyword*
 - **session-state** *keyword*
 - **subscribed-protocols** *string*
 - + **subinterface id** *string*
 - + **admin-state** *keyword*
 - + **desired-minimum-transmit-interval** *number*
 - + **detection-multiplier** *number*
 - + **minimum-echo-receive-interval** *number*
 - + **required-minimum-receive** *number*
 - **total-bfd-sessions** *number*
 - **total-unmatched-bfd-packets** *number*

3.1 bfd Descriptions

bfd

Context	bfd
Tree	bfd
Description	Context to configure BFD parameters and report BFD sessions state
Configurable	True

micro-bfd-sessions



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions
Tree	micro-bfd-sessions
Description	Context to configure micro-BFD session parameters and report sessions state
Configurable	True

lag-interface *name reference*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface <i>name reference</i>
Tree	lag-interface
Description	List of ethernet interface references to associate a micro-BFD session config and state
Configurable	True

name reference



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i>
Description	Reference ID for associated lag interface Example: lag1 (Reference Interface lag1).
Reference	interface name <i>string</i>
Configurable	True

admin-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable BFD for this subinterface
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

desired-minimum-transmit-interval *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> desired-minimum-transmit-interval <i>number</i>
Tree	desired-minimum-transmit-interval
Description	The minimum interval between transmission of BFD control packets This value is advertised to the peer, however the actual interval used is specified by taking the maximum of desired-minimum-transmit-interval and the value of the remote required-minimum-receive interval value. This value is specified as an integer number of microseconds.
Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True

detection-multiplier *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> detection-multiplier <i>number</i>
Tree	detection-multiplier
Description	The number of packets that must be missed to declare this session as down The detection interval for the BFD session is calculated by multiplying the value of the negotiated transmission interval by this value.
Range	3 to 20
Default	3
Configurable	True

local-address (*ipv4-address | ipv6-address*)



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> local-address (<i>ipv4-address ipv6-address</i>)
Tree	local-address
Description	IP address to be used as source address in BFD packets
Configurable	True

member-interface **name** *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i>
Tree	member-interface
Description	List of ethernet interface references to associate a micro-BFD session config and state
Configurable	False

name *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference member-interface name string</i>
Description	Reference ID for associated ethernet interface Example: ethernet-2/1 (Reference Interface ethernet-2/1).
Configurable	False

active-receive-interval *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference member-interface name string active-receive-interval number</i>
Tree	active-receive-interval
Description	The receive interval currently being used by this BFD session This is the amount of time the BFD state machine expects between receiving BFD messages from the remote peer.
Configurable	False

active-transmit-interval *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference member-interface name string active-transmit-interval number</i>
Tree	active-transmit-interval
Description	The transmit interval currently being used by this BFD session This is the amount of time the local BFD agent will wait between the sending of BFD messages to the remote peer
Configurable	False

async



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async
Tree	async
Description	Container for async BFD operational state parameters
Configurable	False

last-clear *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the session counters were cleared.
Configurable	False

last-packet-received *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async last-packet-received <i>string</i>
Tree	last-packet-received
Description	Timestamp for when the last BFD packet was received for this session
Configurable	False

last-packet-transmitted *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async last-packet-transmitted <i>string</i>
Tree	last-packet-transmitted
Description	Timestamp for when the last BFD packet was transmitted for this session
Configurable	False

received-errored-packets *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async received-errored-packets <i>number</i>
Tree	received-errored-packets
Description	Counter for the number of BFD packets received with BFD level errors
Default	0
Configurable	False

received-packets *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async received-packets <i>number</i>
Tree	received-packets
Description	Counter for the number of BFD packets received for this session
Default	0
Configurable	False

transmitted-packets *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async transmitted-packets <i>number</i>
Tree	transmitted-packets
Description	Counter for the number of BFD packets transmitted for this session
Default	0
Configurable	False

up-transitions *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async up-transitions <i>number</i>
Tree	up-transitions
Description	Counter for the number of UP transitions for this BFD session
Default	0
Configurable	False

failure-transitions *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> failure-transitions <i>number</i>
Tree	failure-transitions
Description	The number of times that the BFD session has transitioned out of the up state
Configurable	False

last-failure-time *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> last-failure-time <i>string</i>
Tree	last-failure-time
Description	Timestamp of the last BFD session transition out of the up state to down state
Configurable	False

last-state-transition *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> last-state-transition <i>string</i>
Tree	last-state-transition
Description	Timestamp of the last micro-BFD session transition from any state to any state Time of the session in the current state can be calculated from this value.
Configurable	False

local-diagnostic-code *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> local-diagnostic-code <i>keyword</i>
Tree	local-diagnostic-code
Description	The local BFD diagnostic code indicating the most recent reason for failure of this BFD session
Options	<ul style="list-style-type: none">• NO_DIAGNOSTIC No diagnostic code was specified, or the session has not changed state• DETECTION_TIMEOUT

- The control detection time expired: no BFD packet was received within the required period
- ECHO_FAILED
The BFD echo function failed - echo packets have not been received for the required period of time
 - NEIGHBOR_SIGNED_DOWN
The neighbor signaled session down
 - FORWARDING_RESET
The forwarding plane in the local system was reset
The remote system cannot rely on the forwarding state of the device specifying this error code.
 - PATH_DOWN
Signalling outside of BFD specified that the path underlying this session has failed
 - CONCATENATED_PATH_DOWN
A segment on the path between source and destination has failed
When a BFD session runs over a series of path segments, this error code indicates that a subsequent path segment (i.e., one in the transmit path between the source and destination of the session) has failed.
 - ADMIN_DOWN
The BFD session has been administratively disabled by the peer
 - REVERSE_CONCATENATED_PATH_DOWN
A segment on the reverse path between destination and source has failed
In the case that a BFD session is running over a series of path segments, this error code indicates that a path segment on the reverse path (i.e., in the transmit direction from the destination to the source of the session) has failed.

Configurable False

local-discriminator *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **bfd micro-bfd-sessions lag-interface name** *reference* **member-interface name** *string*
local-discriminator *number*

Tree **local-discriminator**

Description BFD session local discriminator

Configurable False

remote-control-plane-independent *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> remote-control-plane-independent <i>boolean</i>
Tree	remote-control-plane-independent
Description	Indicates if the remote neighbor has set the control independent flag
Configurable	False

remote-diagnostic-code *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> remote-diagnostic-code <i>keyword</i>
Tree	remote-diagnostic-code
Description	The remote BFD diagnostic code indicating the remote system's reason for failure of the BFD session
Options	<ul style="list-style-type: none">• NO_DIAGNOSTIC No diagnostic code was specified, or the session has not changed state• DETECTION_TIMEOUT The control detection time expired: no BFD packet was received within the required period• ECHO_FAILED The BFD echo function failed - echo packets have not been received for the required period of time• NEIGHBOR_SIGNED_DOWN The neighbor signaled session down• FORWARDING_RESET The forwarding plane in the local system was reset The remote system cannot rely on the forwarding state of the device specifying this error code.• PATH_DOWN Signalling outside of BFD specified that the path underlying this session has failed• CONCATENATED_PATH_DOWN A segment on the path between source and destination has failed

When a BFD session runs over a series of path segments, this error code indicates that a subsequent path segment (i.e., one in the transmit path between the source and destination of the session) has failed.

- ADMIN_DOWN

The BFD session has been administratively disabled by the peer

- REVERSE_CONCATENATED_PATH_DOWN

A segment on the reverse path between destination and source has failed

In the case that a BFD session is running over a series of path segments, this error code indicates that a path segment on the reverse path (i.e., in the transmit direction from the destination to the source of the session) has failed.

Configurable False

remote-discriminator *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **bfd micro-bfd-sessions lag-interface name** *reference* **member-interface name** *string*
remote-discriminator *number*

Tree **remote-discriminator**

Description A unique identifier used by the remote system to identify this BFD session

Configurable False

remote-minimum-receive-interval *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **bfd micro-bfd-sessions lag-interface name** *reference* **member-interface name** *string*
remote-minimum-receive-interval *number*

Tree **remote-minimum-receive-interval**

Description The value of the minimum receive interval that was specified by the peer
This value references the value in the most recent BFD control packet received from the peer.

Configurable False

remote-multiplier *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> remote-multiplier <i>number</i>
Tree	remote-multiplier
Description	The current number of packets that must be missed to declare the session as down The detection interval for the BFD session is calculated by multiplying the value of the negotiated transmission interval by this value.
Configurable	False

remote-session-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> remote-session-state <i>keyword</i>
Tree	remote-session-state
Description	The reported state of the BFD session according to the remote system This state reflects the last state reported in a BFD control packet.
Options	<ul style="list-style-type: none">• ADMIN_DOWN The BFD session is administratively disabled• DOWN The BFD session is perceived to be down by the system• INIT The BFD session is perceived to be initialising by the system• UP The BFD session is perceived to be up by the system
Configurable	False

session-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> session-state <i>keyword</i>
Tree	session-state
Description	The state of the BFD session perceived by the local system
Options	<ul style="list-style-type: none">• ADMIN_DOWN The BFD session is administratively disabled• DOWN The BFD session is perceived to be down by the system• INIT The BFD session is perceived to be initialising by the system• UP The BFD session is perceived to be up by the system
Configurable	False

remote-address (*ipv4-address | ipv6-address*)



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> remote-address (<i>ipv4-address ipv6-address</i>)
Tree	remote-address
Description	The remote IP address for the far-end of the BFD session This must be the same IP version as the local-address.
Configurable	True

required-minimum-receive *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> required-minimum-receive number
Tree	required-minimum-receive
Description	The minimum interval between received BFD control packets that this system should support This value is advertised to the remote peer to indicate the maximum frequency (i.e., minimum inter-packet interval) between BFD control packets that is acceptable to the local system. This value is specified as an integer number of microseconds.
Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True

network-instance name *string*

Context	bfd network-instance name <i>string</i>
Tree	network-instance
Description	network-instance context for BFD session.
Configurable	False

name *string*

Context	bfd network-instance name <i>string</i>
Description	A unique name identifying the network instance
Configurable	False

peer local-discriminator *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i>
Tree	peer
Description	BFD session state related to this peer
Configurable	False

local-discriminator *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i>
Description	BFD session local discriminator
Configurable	False

active-receive-interval *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> active-receive-interval <i>number</i>
Tree	active-receive-interval
Description	The receive interval currently being used by this BFD session This is the amount of time the BFD state machine expects between receiving BFD messages from the remote peer.
Configurable	False

active-transmit-interval *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> active-transmit-interval <i>number</i>
Tree	active-transmit-interval
Description	The transmit interval currently being used by this BFD session This is the amount of time the local BFD agent will wait between the sending of BFD messages to the remote peer
Configurable	False

async

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async
Tree	async
Description	Container for async BFD operational state parameters
Configurable	False

last-clear *string*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the session counters were cleared.
Configurable	False

last-packet-received *string*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async last-packet-received <i>string</i>
Tree	last-packet-received
Description	Timestamp for when the last BFD packet was received for this session
Configurable	False

last-packet-transmitted *string*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async last-packet-transmitted <i>string</i>
Tree	last-packet-transmitted
Description	Timestamp for when the last BFD packet was transmitted for this session
Configurable	False

received-errored-packets *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async received-errored-packets <i>number</i>
Tree	received-errored-packets
Description	Counter for the number of BFD packets received with BFD level errors
Default	0
Configurable	False

received-packets *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async received-packets <i>number</i>
Tree	received-packets
Description	Counter for the number of BFD packets received for this session
Default	0
Configurable	False

transmitted-packets *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async transmitted-packets <i>number</i>
Tree	transmitted-packets
Description	Counter for the number of BFD packets transmitted for this session
Default	0
Configurable	False

up-transitions *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async up-transitions <i>number</i>
Tree	up-transitions
Description	Counter for the number of UP transitions for this BFD session
Default	0
Configurable	False

failure-transitions *number*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> failure-transitions <i>number</i>
Tree	failure-transitions
Description	The number of times that the BFD session has transitioned out of the up state
Configurable	False

last-failure-time *string*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> last-failure-time <i>string</i>
Tree	last-failure-time
Description	Timestamp of the last BFD session transition out of the up state to down state
Configurable	False

last-state-transition *string*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> last-state-transition <i>string</i>
Tree	last-state-transition
Description	Timestamp of the last BFD session transition from any state to any state Time of the session in the current state can be calculated from this value.
Configurable	False

local-address (*ipv4-address | ipv6-address*)

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> local-address (<i>ipv4-address ipv6-address</i>)
Tree	local-address
Description	IP address to be used as source address in BFD packets
Configurable	False

local-diagnostic-code *keyword*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> local-diagnostic-code <i>keyword</i>
Tree	local-diagnostic-code
Description	The local BFD diagnostic code indicating the most recent reason for failure of this BFD session
Options	<ul style="list-style-type: none">• NO_DIAGNOSTIC No diagnostic code was specified, or the session has not changed state• DETECTION_TIMEOUT The control detection time expired: no BFD packet was received within the required period• ECHO_FAILED The BFD echo function failed - echo packets have not been received for the required period of time• NEIGHBOR_SIGNED_DOWN The neighbor signaled session down• FORWARDING_RESET The forwarding plane in the local system was reset The remote system cannot rely on the forwarding state of the device specifying this error code.• PATH_DOWN Signalling outside of BFD specified that the path underlying this session has failed• CONCATENATED_PATH_DOWN

A segment on the path between source and destination has failed

When a BFD session runs over a series of path segments, this error code indicates that a subsequent path segment (i.e., one in the transmit path between the source and destination of the session) has failed.

- ADMIN_DOWN

The BFD session has been administratively disabled by the peer

- REVERSE_CONCATENATED_PATH_DOWN

A segment on the reverse path between destination and source has failed

In the case that a BFD session is running over a series of path segments, this error code indicates that a path segment on the reverse path (i.e., in the transmit direction from the destination to the source of the session) has failed.

Configurable False

oper-state keyword

Context **bfd network-instance name** *string* **peer local-discriminator** *number* **oper-state** *keyword*

Tree **oper-state**

Description Details the operational state of the session

- Options
- up
Component or process is operational
 - down
Component or process is not operational
 - empty
Component slot is empty
 - downloading
Component is downloading image into memory
 - booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing
Component is currently being synchronized
 - upgrading
Component is currently being upgraded

Configurable False

remote-address (*ipv4-address | ipv6-address*)

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>)
Tree	remote-address
Description	The remote IP address for the far-end of the BFD session This must be the same IP version as the local-address.
Configurable	False

remote-control-plane-independent *boolean*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-control-plane-independent <i>boolean</i>
Tree	remote-control-plane-independent
Description	Indicates if the remote neighbor has set the control independent flag
Configurable	False

remote-diagnostic-code *keyword*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-diagnostic-code <i>keyword</i>
Tree	remote-diagnostic-code
Description	The remote BFD diagnostic code indicating the remote system's reason for failure of the BFD session
Options	<ul style="list-style-type: none">• NO_DIAGNOSTIC No diagnostic code was specified, or the session has not changed state• DETECTION_TIMEOUT The control detection time expired: no BFD packet was received within the required period• ECHO_FAILED The BFD echo function failed - echo packets have not been received for the required period of time• NEIGHBOR_SIGNED_DOWN The neighbor signaled session down• FORWARDING_RESET The forwarding plane in the local system was reset The remote system cannot rely on the forwarding state of the device specifying this error code.• PATH_DOWN Signalling outside of BFD specified that the path underlying this session has failed• CONCATENATED_PATH_DOWN

A segment on the path between source and destination has failed

When a BFD session runs over a series of path segments, this error code indicates that a subsequent path segment (i.e., one in the transmit path between the source and destination of the session) has failed.

- ADMIN_DOWN

The BFD session has been administratively disabled by the peer

- REVERSE_CONCATENATED_PATH_DOWN

A segment on the reverse path between destination and source has failed

In the case that a BFD session is running over a series of path segments, this error code indicates that a path segment on the reverse path (i.e., in the transmit direction from the destination to the source of the session) has failed.

Configurable False

remote-discriminator *number*

Context **bfd network-instance name** *string* **peer local-discriminator** *number* **remote-discriminator** *number*

Tree **remote-discriminator**

Description A unique identifier used by the remote system to identify this BFD session

Configurable False

remote-minimum-receive-interval *number*

Context **bfd network-instance name** *string* **peer local-discriminator** *number* **remote-minimum-receive-interval** *number*

Tree **remote-minimum-receive-interval**

Description The value of the minimum receive interval that was specified by the peer

This value references the value in the most recent BFD control packet received from the peer.

Configurable False

remote-multiplier *number*

Context **bfd network-instance name** *string* **peer local-discriminator** *number* **remote-multiplier** *number*

Tree **remote-multiplier**

Description The current number of packets that must be missed to declare the session as down

The detection interval for the BFD session is calculated by multiplying the value of the negotiated transmission interval by this value.

Configurable False

remote-session-state *keyword*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-session-state <i>keyword</i>
Tree	remote-session-state
Description	The reported state of the BFD session according to the remote system This state reflects the last state reported in a BFD control packet.
Options	<ul style="list-style-type: none">• ADMIN_DOWN The BFD session is administratively disabled• DOWN The BFD session is perceived to be down by the system• INIT The BFD session is perceived to be initialising by the system• UP The BFD session is perceived to be up by the system
Configurable	False

session-state *keyword*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> session-state <i>keyword</i>
Tree	session-state
Description	The state of the BFD session perceived by the local system
Options	<ul style="list-style-type: none">• ADMIN_DOWN The BFD session is administratively disabled• DOWN The BFD session is perceived to be down by the system• INIT The BFD session is perceived to be initialising by the system• UP The BFD session is perceived to be up by the system
Configurable	False

subscribed-protocols *string*

Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> subscribed-protocols <i>string</i>
Tree	subscribed-protocols
Description	Indicates the set of protocols that currently use this BFD session for liveness detection
Configurable	False

subinterface id *string*

Context	bfd subinterface id <i>string</i>
Tree	subinterface
Description	List of subinterface references to associating BFD config and state
Configurable	True

id *string*

Context	bfd subinterface id <i>string</i>
Description	Reference ID for associated subinterface Example: ethernet-2/1.100 (Reference Interface ethernet-2/1, subinterface 100).
String Length	3 to 24
Configurable	True

admin-state *keyword*

Context	bfd subinterface id <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable BFD for this subinterface
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

desired-minimum-transmit-interval *number*

Context	bfd subinterface id <i>string</i> desired-minimum-transmit-interval <i>number</i>
Tree	desired-minimum-transmit-interval
Description	The minimum interval between transmission of BFD control packets

This value is advertised to the peer, however the actual interval used is specified by taking the maximum of desired-minimum-transmit-interval and the value of the remote required-minimum-receive interval value. This value is specified as an integer number of microseconds.

Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True

detection-multiplier *number*

Context	bfd subinterface id <i>string</i> detection-multiplier <i>number</i>
Tree	detection-multiplier
Description	The number of packets that must be missed to declare this session as down The detection interval for the BFD session is calculated by multiplying the value of the negotiated transmission interval by this value.
Range	3 to 20
Default	3
Configurable	True

minimum-echo-receive-interval *number*

Context	bfd subinterface id <i>string</i> minimum-echo-receive-interval <i>number</i>
Tree	minimum-echo-receive-interval
Description	The minimum interval between echo packets the local node can receive Implicitly enabled echo mode on the associated interface.
Range	0 250000 to 100000000
Default	0
Configurable	True

required-minimum-receive *number*

Context	bfd subinterface id <i>string</i> required-minimum-receive <i>number</i>
Tree	required-minimum-receive
Description	The minimum interval between received BFD control packets that this system should support

This value is advertised to the remote peer to indicate the maximum frequency (i.e., minimum inter-packet interval) between BFD control packets that is acceptable to the local system. This value is specified as an integer number of microseconds.

Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True

total-bfd-sessions *number*

Context	bfd total-bfd-sessions <i>number</i>
Tree	total-bfd-sessions
Description	Counter for the total number of BFD sessions
Default	0
Configurable	False

total-unmatched-bfd-packets *number*

Context	bfd total-unmatched-bfd-packets <i>number</i>
Tree	total-unmatched-bfd-packets
Description	Counter for the total number of BFD packets received not matching a BFD session
Default	0
Configurable	False

4 interface

interface name *string*

- + **admin-state** *keyword*
- + **description** *string*
- + **ethernet**
 - + **aggregate-id** *reference*
 - + **flow-control**
 - + **receive** *boolean*
 - **hw-mac-address** *string*
 - + **port-speed** *keyword*
 - **statistics**
 - **in-1024b-to-1518b-frames** *number*
 - **in-128b-to-255b-frames** *number*
 - **in-1519b-or-longer-frames** *number*
 - **in-256b-to-511b-frames** *number*
 - **in-512b-to-1023b-frames** *number*
 - **in-64b-frames** *number*
 - **in-65b-to-127b-frames** *number*
 - **in-crc-error-frames** *number*
 - **in-fragment-frames** *number*
 - **in-jabber-frames** *number*
 - **in-mac-pause-frames** *number*
 - **in-oversize-frames** *number*
 - **last-clear** *string*
 - **out-1024b-to-1518b-frames** *number*
 - **out-128b-to-255b-frames** *number*
 - **out-1519b-or-longer-frames** *number*
 - **out-256b-to-511b-frames** *number*
 - **out-512b-to-1023b-frames** *number*
 - **out-64b-frames** *number*
 - **out-65b-to-127b-frames** *number*
 - **out-mac-pause-frames** *number*
- **ifindex** *number*
- + **lag**
 - + **lacp**
 - + **admin-key** *number*
 - + **interval** *keyword*
 - + **lacp-mode** *keyword*
 - + **system-id-mac** *string*
 - + **system-priority** *number*
 - **lag-speed** *number*
 - + **lag-type** *keyword*
 - **members name** *reference*
 - **activity** *keyword*
 - **aggregatable** *boolean*
 - **collecting** *boolean*
 - **distributing** *boolean*
 - **microbfd-enabled** *boolean*
 - **oper-down-reason** *keyword*
 - **oper-key** *number*
 - **oper-state** *keyword*

- **partner-id** *string*
- **partner-key** *number*
- **partner-port-num** *number*
- **port-num** *number*
- **statistics**
 - **lACP-errors** *number*
 - **lACP-in-pkts** *number*
 - **lACP-out-pkts** *number*
 - **lACP-rx-errors** *number*
 - **lACP-tx-errors** *number*
 - **lACP-unknown-errors** *number*
- **synchronization** *keyword*
- **system-id** *string*
- **timeout** *keyword*
- + **min-links** *number*
- **last-change** *string*
- + **loopback-mode** *boolean*
- + **mtu** *number*
- **oper-down-reason** *keyword*
- **oper-state** *keyword*
- + **qos**
 - + **output**
 - + **unicast-queue queue-id** *number*
 - + **queue-parameters**
 - **peak-rate-bps** *number*
 - + **peak-rate-percent** *number*
 - + **strict-priority** *boolean*
 - + **weight** *number*
- **queue-statistics**
 - **multicast-queue queue-id** *number*
 - **final-dropped-octets** *number*
 - **final-dropped-packets** *number*
 - **last-clear** *string*
 - **transmitted-octets** *number*
 - **transmitted-packets** *number*
 - **unicast-queue queue-id** *number*
 - **final-dropped-octets** *number*
 - **final-dropped-packets** *number*
 - **last-clear** *string*
 - **transmitted-octets** *number*
 - **transmitted-packets** *number*
 - **virtual-output-queue slot** *number*
 - **dropped-octets** *number*
 - **dropped-packets** *number*
 - **forwarded-octets** *number*
 - **forwarded-packets** *number*
- + **sflow**
 - + **admin-state** *keyword*
- **statistics**
 - **carrier-transitions** *number*
 - **in-broadcast-packets** *number*
 - **in-error-packets** *number*
 - **in-fcs-error-packets** *number*
 - **in-multicast-packets** *number*

- **in-octets** *number*
- **in-unicast-packets** *number*
- **last-clear** *string*
- **out-broadcast-packets** *number*
- **out-error-packets** *number*
- **out-multicast-packets** *number*
- **out-octets** *number*
- **out-unicast-packets** *number*
- + **subinterface index** *number*
- + **acl**
 - + **input**
 - + **ipv4-filter** *reference*
 - + **ipv6-filter** *reference*
 - + **output**
 - + **ipv4-filter** *reference*
 - + **ipv6-filter** *reference*
- + **admin-state** *keyword*
- + **bridge-table**
 - + **discard-unknown-src-mac** *boolean*
 - + **mac-duplication**
 - + **action** *keyword*
 - + **mac-learning**
 - + **admin-state** *keyword*
 - + **aging**
 - + **admin-state** *keyword*
 - + **mac-limit**
 - + **maximum-entries** *number*
 - + **warning-threshold-pct** *number*
 - **statistics**
 - **active-entries** *number*
 - **mac-type type** *keyword*
 - **active-entries** *number*
 - **total-entries** *number*
 - **total-entries** *number*
- + **description** *string*
- + **ip-mtu** *number*
- + **ipv4**
 - + **address ip-prefix** *string*
 - **origin** *keyword*
 - **status** *keyword*
 - + **vrrp**
 - + **vrrp-group virtual-router-id** *number*
 - + **accept-mode** *boolean*
 - + **advertise-interval** *number*
 - + **authentication**
 - + **text-key** *string*
 - + **type** *keyword*
 - + **init-delay** *number*
 - + **interface-tracking**
 - + **priority-decrement** *number*
 - + **track-interface** *reference*
 - + **preempt** *boolean*
 - + **preempt-delay** *number*
 - + **priority** *number*

- + **state**
 - **operational-priority** *number*
- + **version** *number*
- + **virtual-address** (*ipv4-address* | *ipv6-address*)
- + **allow-directed-broadcast** *boolean*
- + **arp**
 - + **neighbor ipv4-address** *string*
 - **expiration-time** *string*
 - + **link-layer-address** *string*
 - **origin** *keyword*
 - + **timeout** *number*
- + **dhcp-client**
 - + **trace-options**
 - + **trace** *keyword*
- + **dhcp-relay**
 - + **option** *keyword*
 - + **server** (*ipv4-address* | *domain-name*)
 - + **source-address** *string*
 - + **trace-options**
 - + **trace** *keyword*
- + **ipv6**
 - + **address ip-prefix** *string*
 - **origin** *keyword*
 - **status** *keyword*
 - + **vrrp**
 - + **vrrp-group virtual-router-id** *number*
 - + **accept-mode** *boolean*
 - + **advertise-interval** *number*
 - + **authentication**
 - + **text-key** *string*
 - + **type** *keyword*
 - + **init-delay** *number*
 - + **interface-tracking**
 - + **priority-decrement** *number*
 - + **track-interface** *reference*
 - + **preempt** *boolean*
 - + **preempt-delay** *number*
 - + **priority** *number*
 - + **state**
 - **operational-priority** *number*
 - + **version** *number*
 - + **virtual-address** (*ipv4-address* | *ipv6-address*)
 - + **dhcp-client**
 - + **trace-options**
 - + **trace** *keyword*
 - + **dhcp-relay**
 - + **option** *keyword*
 - + **server** (*ipv6-address* | *domain-name*)
 - + **source-address** *string*
 - + **trace-options**
 - + **trace** *keyword*
 - + **neighbor-discovery**
 - + **duplicate-address-detection** *boolean*
 - + **neighbor ipv6-address** *string*

- **current-state** *keyword*
- **is-router** *boolean*
- + **link-layer-address** *string*
- **next-state-time** *string*
- **origin** *keyword*
- + **reachable-time** *number*
- + **stale-time** *number*
- + **router-advertisement**
 - + **router-role**
 - + **admin-state** *keyword*
 - + **current-hop-limit** *number*
 - + **ip-mtu** *number*
 - + **managed-configuration-flag** *boolean*
 - + **max-advertisement-interval** *number*
 - + **min-advertisement-interval** *number*
 - + **other-configuration-flag** *boolean*
 - + **prefix ipv6-prefix** *string*
 - + **autonomous-flag** *boolean*
 - + **on-link-flag** *boolean*
 - + **preferred-lifetime** (*keyword* | *number*)
 - + **valid-lifetime** (*keyword* | *number*)
 - + **reachable-time** *number*
 - + **retransmit-time** *number*
 - + **router-lifetime** *number*
 - + **trace-options**
 - + **trace** *keyword*
- + **l2-mtu** *number*
- **last-change** *string*
- **name** *string*
- **oper-down-reason** *keyword*
- **oper-state** *keyword*
- + **qos**
 - + **input**
 - + **classifiers**
 - + **dscp** *reference*
 - + **ipv4-dscp** *reference*
 - + **ipv6-dscp** *reference*
 - + **mpls-traffic-class** *reference*
 - + **output**
 - + **rewrite-rules**
 - + **dscp** *reference*
 - + **ipv4-dscp** *reference*
 - + **ipv6-dscp** *reference*
 - + **mpls-traffic-class** *reference*
- **statistics**
 - **in-discarded-packets** *number*
 - **in-error-packets** *number*
 - **in-forwarded-octets** *number*
 - **in-forwarded-packets** *number*
 - **in-octets** *number*
 - **in-packets** *number*
 - **in-terminated-octets** *number*
 - **in-terminated-packets** *number*
 - **last-clear** *string*

- **out-discarded-packets** *number*
- **out-error-packets** *number*
- **out-forwarded-octets** *number*
- **out-forwarded-packets** *number*
- **out-octets** *number*
- **out-originated-octets** *number*
- **out-originated-packets** *number*
- **out-packets** *number*
- + **type** *identityref*
- + **vlan**
 - + **encap**
 - + **single-tagged**
 - + **vlan-id** *number*
- **traffic-rate**
 - **in-bps** *number*
 - **out-bps** *number*
- + **transceiver**
 - + **admin-state** *keyword*
 - **channel index** *number*
 - **input-power**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *decimal-number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *decimal-number*
 - **laser-bias-current**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *decimal-number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *decimal-number*
 - **output-power**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *decimal-number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *decimal-number*
 - **wavelength** *decimal-number*
 - **connector-type** *keyword*
 - **date-code** *string*
 - + **ddm-events** *boolean*
 - **ethernet-pmd** *string*

- **fault-condition** *boolean*
- **form-factor** *keyword*
- + **forward-error-correction** *keyword*
- **input-power**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *decimal-number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *decimal-number*
- **laser-bias-current**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *decimal-number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *decimal-number*
- **oper-state** *keyword*
- **output-power**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *decimal-number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *decimal-number*
- **serial-number** *string*
- **temperature**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *number*
 - **latest-value** *number*
 - **low-alarm-condition** *boolean*
 - **low-alarm-threshold** *number*
 - **low-warning-condition** *boolean*
 - **low-warning-threshold** *number*
- **vendor** *string*
- **vendor-part-number** *string*
- **vendor-revision** *string*
- **voltage**
 - **high-alarm-condition** *boolean*
 - **high-alarm-threshold** *decimal-number*
 - **high-warning-condition** *boolean*
 - **high-warning-threshold** *decimal-number*
 - **latest-value** *decimal-number*

- **low-alarm-condition** *boolean*
- **low-alarm-threshold** *decimal-number*
- **low-warning-condition** *boolean*
- **low-warning-threshold** *decimal-number*
- **wavelength** *decimal-number*
- + **vlan-tagging** *boolean*

4.1 interface Descriptions

interface **name** *string*

Context	interface name <i>string</i>
Tree	interface
Description	The list of named interfaces on the device.
Configurable	True

name *string*

Context	interface name <i>string</i>
Description	The name of the interface Valid options are: mgmt<N>, N=0 mgmt<N>-standby, N=0 lo<N>, N=0..255 lag<N> irb<N>, N=0..255 ethernet-<slot>/<port> ethernet-<slot>/<mda>/<port> ethernet-<slot>/<connector>/<lane> ethernet-<slot>/<mda>/<connector>/<lane> <slot>=slot number {1,2,3,..} <mda>=mda id {a,b,c,d} <connector>=connector id {1,2,3,..} <port>=port id {1,2,3,..} <lane>=channel or breakout port id {1,2,3,..}
String Length	3 to 19
Configurable	True

admin-state *keyword*

Context	interface name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	The configured, desired state of the interface
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

description *string*

Context	interface name <i>string</i> description <i>string</i>
Tree	description
Description	A user-configured description of the interface
String Length	1 to 255
Configurable	True

ethernet

Context	interface name <i>string</i> ethernet
Tree	ethernet
Description	
Configurable	True

aggregate-id *reference*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> ethernet aggregate-id <i>reference</i>
Tree	aggregate-id
Description	lag interface with which this interface is associated.
Reference	interface name <i>string</i>
Configurable	True

flow-control

Context	interface name <i>string</i> ethernet flow-control
Tree	flow-control
Description	
Configurable	True

receive *boolean*

Context	interface name <i>string</i> ethernet flow-control receive <i>boolean</i>
Tree	receive
Description	When this is true PAUSE frames received on this interface are accepted and processed. When this is false PAUSE frames received on this interface are ignored.
Configurable	True

hw-mac-address *string*

Context	interface name <i>string</i> ethernet hw-mac-address <i>string</i>
Tree	hw-mac-address
Description	The MAC address associated with the port
Configurable	False

port-speed *keyword*

Context	interface name <i>string</i> ethernet port-speed <i>keyword</i>
Tree	port-speed
Description	<p>The speed of the port or channel</p> <p>If no value is configured, the value is read from hardware.</p> <p>If a value is configured but the interface corresponds to a slot with no IMM, or an MDA slot with no MDA, or a connector with no transceiver the value is accepted without checking or restriction and it will be displayed as the operational (state) value.</p> <p>If a value is configured and the interface corresponds to an installed IMM, MDA (if applicable) and connector and the port-speed is supported by the installed transceiver then the value is accepted and it will be displayed as the operational (state) value.</p> <p>If a value is configured and the interface corresponds to an installed IMM, MDA (if applicable) and connector and the port-speed is NOT supported by the installed transceiver then the port is forced operationally down.</p>
Options	<ul style="list-style-type: none">• 10M• 100M• 1G• 10G• 25G• 40G• 50G• 100G• 200G• 400G

Configurable • 1T
 True

statistics

Context [interface name](#) *string* [ethernet statistics](#)
Tree [statistics](#)
Description
Configurable False

in-1024b-to-1518b-frames *number*

Context [interface name](#) *string* [ethernet statistics in-1024b-to-1518b-frames](#) *number*
Tree [in-1024b-to-1518b-frames](#)
Description Number of received Ethernet frames that are 1024-1518 bytes in length
Default 0
Configurable False

in-128b-to-255b-frames *number*

Context [interface name](#) *string* [ethernet statistics in-128b-to-255b-frames](#) *number*
Tree [in-128b-to-255b-frames](#)
Description Number of received Ethernet frames that are 128-255 bytes in length
Default 0
Configurable False

in-1519b-or-longer-frames *number*

Context [interface name](#) *string* [ethernet statistics in-1519b-or-longer-frames](#) *number*
Tree [in-1519b-or-longer-frames](#)
Description Number of received Ethernet frames that are 1519 bytes or longer
Default 0
Configurable False

in-256b-to-511b-frames *number*

Context	interface name <i>string</i> ethernet statistics in-256b-to-511b-frames <i>number</i>
Tree	in-256b-to-511b-frames
Description	Number of received Ethernet frames that are 256-511 bytes in length
Default	0
Configurable	False

in-512b-to-1023b-frames *number*

Context	interface name <i>string</i> ethernet statistics in-512b-to-1023b-frames <i>number</i>
Tree	in-512b-to-1023b-frames
Description	Number of received Ethernet frames that are 512-1023 bytes in length
Default	0
Configurable	False

in-64b-frames *number*

Context	interface name <i>string</i> ethernet statistics in-64b-frames <i>number</i>
Tree	in-64b-frames
Description	Number of received Ethernet frames that are exactly 64 bytes in length
Default	0
Configurable	False

in-65b-to-127b-frames *number*

Context	interface name <i>string</i> ethernet statistics in-65b-to-127b-frames <i>number</i>
Tree	in-65b-to-127b-frames
Description	Number of received Ethernet frames that are 65-127 bytes in length
Default	0
Configurable	False

in-crc-error-frames *number*

Context	interface name <i>string</i> ethernet statistics in-crc-error-frames <i>number</i>
Tree	in-crc-error-frames
Description	Number of receive error events due to FCS/CRC check failure.
Default	0
Configurable	False

in-fragment-frames *number*

Context	interface name <i>string</i> ethernet statistics in-fragment-frames <i>number</i>
Tree	in-fragment-frames
Description	Number of fragment frames received on the interface.
Default	0
Configurable	False

in-jabber-frames *number*

Context	interface name <i>string</i> ethernet statistics in-jabber-frames <i>number</i>
Tree	in-jabber-frames
Description	Number of jabber frames received on the interface. Jabber frames are typically defined as oversize frames which also have a bad CRC.
Default	0
Configurable	False

in-mac-pause-frames *number*

Context	interface name <i>string</i> ethernet statistics in-mac-pause-frames <i>number</i>
Tree	in-mac-pause-frames
Description	Number of MAC layer PAUSE frames received on the interface.
Default	0
Configurable	False

in-oversize-frames *number*

Context	interface name <i>string</i> ethernet statistics in-oversize-frames <i>number</i>
Tree	in-oversize-frames
Description	Number of oversize frames received on the interface (i.e. frames that exceed the operational port MTU)
Default	0
Configurable	False

last-clear *string*

Context	interface name <i>string</i> ethernet statistics last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the MAC counters were cleared.
Configurable	False

out-1024b-to-1518b-frames *number*

Context	interface name <i>string</i> ethernet statistics out-1024b-to-1518b-frames <i>number</i>
Tree	out-1024b-to-1518b-frames
Description	Number of transmitted Ethernet frames that are 1024-1518 bytes in length
Default	0
Configurable	False

out-128b-to-255b-frames *number*

Context	interface name <i>string</i> ethernet statistics out-128b-to-255b-frames <i>number</i>
Tree	out-128b-to-255b-frames
Description	Number of transmitted Ethernet frames that are 128-255 bytes in length
Default	0
Configurable	False

out-1519b-or-longer-frames *number*

Context	interface name <i>string</i> ethernet statistics out-1519b-or-longer-frames <i>number</i>
Tree	out-1519b-or-longer-frames
Description	Number of transmitted Ethernet frames that are 1519 bytes or longer
Default	0
Configurable	False

out-256b-to-511b-frames *number*

Context	interface name <i>string</i> ethernet statistics out-256b-to-511b-frames <i>number</i>
Tree	out-256b-to-511b-frames
Description	Number of transmitted Ethernet frames that are 256-511 bytes in length
Default	0
Configurable	False

out-512b-to-1023b-frames *number*

Context	interface name <i>string</i> ethernet statistics out-512b-to-1023b-frames <i>number</i>
Tree	out-512b-to-1023b-frames
Description	Number of transmitted Ethernet frames that are 512-1023 bytes in length
Default	0
Configurable	False

out-64b-frames *number*

Context	interface name <i>string</i> ethernet statistics out-64b-frames <i>number</i>
Tree	out-64b-frames
Description	Number of transmitted Ethernet frames that are exactly 64 bytes in length
Default	0
Configurable	False

out-65b-to-127b-frames *number*

Context	interface name <i>string</i> ethernet statistics out-65b-to-127b-frames <i>number</i>
Tree	out-65b-to-127b-frames
Description	Number of transmitted Ethernet frames that are 65-127 bytes in length
Default	0
Configurable	False

out-mac-pause-frames *number*

Context	interface name <i>string</i> ethernet statistics out-mac-pause-frames <i>number</i>
Tree	out-mac-pause-frames
Description	Number of MAC layer PAUSE frames sent on the interface.
Default	0
Configurable	False

ifindex *number*

Context	interface name <i>string</i> ifindex <i>number</i>
Tree	ifindex
Description	System-wide persistent unique ifIndex assigned to the interface
Configurable	False

lag



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag
Tree	lag
Description	Container for options related to LAG
Configurable	True

lACP



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string lag lACP</i>
Tree	lACP
Description	LACP parameters for the associated LAG
Configurable	True

admin-key *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string lag lACP admin-key number</i>
Tree	admin-key
Description	Configure the LACP admin-key to be advertised by the local system. If this value is not specified a value starting from 32768 is automatically assigned by the system.
Range	1 to 65535
Configurable	True

interval *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string lag lACP interval keyword</i>
Tree	interval
Description	Set the period between LACP messages -- uses the lACP-period-type enumeration.
Default	SLOW
Options	<ul style="list-style-type: none">• FAST Send LACP packets every second• SLOW

Send LACP packets every 30 seconds

Configurable True

lACP-mode *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string lag lACP lACP-mode keyword*

Tree **lACP-mode**

Description ACTIVE is to initiate the transmission of LACP packets. PASSIVE is to wait for peer to initiate the transmission of LACP packets.

Default ACTIVE

- Options
- ACTIVE
Interface is an active member, i.e., will detect and maintain aggregates
 - PASSIVE
Interface is a passive member, i.e., it participates with an active partner

Configurable True

system-id-mac *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string lag lACP system-id-mac string*

Tree **system-id-mac**

Description The MAC address portion of the node's System ID. This is combined with the system priority to construct the 8-octet system-id. If not configured, the system-ID configured at the system/level is used.

Configurable True

system-priority *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag lacp system-priority <i>number</i>
Tree	system-priority
Description	System priority used by the node on this LAG interface. Lower value is higher priority for determining which node is the controlling system. If not configured, the system-priority configured at the system/level is used.
Configurable	True

lag-speed *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag lag-speed <i>number</i>
Tree	lag-speed
Description	Reports current aggregate bandwidth speed of the associated LAG
Units	Mbps
Configurable	False

lag-type *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag lag-type <i>keyword</i>
Tree	lag-type
Description	Sets the type of LAG, i.e., how it is configured /maintained
Default	static
Options	<ul style="list-style-type: none">• lacp LAG managed by LACP• static

Statically configured bundle / LAG

Configurable True

members **name** *reference*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string lag members name* *reference*

Tree **members**

Description Reports the list of interfaces associated with the LAG instance

Configurable False

name *reference*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string lag members name* *reference*

Description

Reference **interface name** *string*

Configurable False

activity *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string lag members name* *reference* **activity** *keyword*

Tree **activity**

Description Indicates participant is active or passive

- Options
- ACTIVE
Interface is an active member, i.e., will detect and maintain aggregates
 - PASSIVE

Interface is a passive member, i.e., it participates with an active partner

Configurable False

aggregatable *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string* **lag members name** *reference* **aggregatable** *boolean*

Tree **aggregatable**

Description A true value indicates that the participant will allow the link to be used as part of the aggregate. A false value indicates the link should be used as an individual link

Configurable False

collecting *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string* **lag members name** *reference* **collecting** *boolean*

Tree **collecting**

Description If true, the participant is collecting incoming frames on the link, otherwise false

Configurable False

distributing *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string* **lag members name** *reference* **distributing** *boolean*

Tree **distributing**

Description When true, the participant is distributing outgoing frames; when false, distribution is disabled

Configurable False

microbfd-enabled *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> microbfd-enabled <i>boolean</i>
Tree	microbfd-enabled
Description	Indicates if microBFD is currently used in the determination of the member-link oper-status
Configurable	False

oper-down-reason *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Description	Reason for operational down state for the associated LAG
Options	<ul style="list-style-type: none">• port-admin-disabled• port-oper-disabled• lag-admin-disabled• lacp-down• microBFD-down• lag-min-link-threshold• other
Configurable	False

oper-key *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> oper-key <i>number</i>
Tree	oper-key
Description	Current operational value of the key for the aggregate interface
Configurable	False

oper-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
Description	Operational state for the associated LAG
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

partner-id *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> partner-id <i>string</i>
Tree	partner-id
Description	MAC address representing the protocol partner's interface system ID
Configurable	False

partner-key *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> partner-key <i>number</i>
Tree	partner-key
Description	Operational value of the protocol partner's key
Configurable	False

partner-port-num *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> partner-port-num <i>number</i>
Tree	partner-port-num
Description	Port number of the partner (remote) port for this member port
Configurable	False

port-num *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> port-num <i>number</i>
Tree	port-num
Description	Port number of the local (actor) aggregation member
Configurable	False

statistics



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics
Tree	statistics
Description	LACP protocol counters
Configurable	False

lACP-errors *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics lACP-errors <i>number</i>
Tree	lACP-errors
Description	Number of LACPDU illegal packet errors
Default	0
Configurable	False

lACP-in-pkts *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics lACP-in-pkts <i>number</i>
Tree	lACP-in-pkts
Description	Number of LACPDU received
Default	0
Configurable	False

lACP-out-pkts *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics lACP-out-pkts <i>number</i>
Tree	lACP-out-pkts
Description	Number of LACPDU transmitted
Default	0
Configurable	False

lACP-rx-errors *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics lACP-rx-errors <i>number</i>
Tree	lACP-rx-errors
Description	Number of LACPDU receive packet errors
Default	0
Configurable	False

lACP-tx-errors *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics lACP-tx-errors <i>number</i>
Tree	lACP-tx-errors
Description	Number of LACPDU transmit packet errors
Default	0
Configurable	False

lACP-unknown-errors *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> statistics lACP-unknown-errors <i>number</i>
Tree	lACP-unknown-errors
Description	Number of LACPDU unknown packet errors
Default	0
Configurable	False

synchronization *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag members name <i>reference</i> synchronization <i>keyword</i>
Tree	synchronization
Description	Indicates whether the participant is in-sync or out-of-sync
Options	<ul style="list-style-type: none">• IN_SYNC Participant is in sync with the system id and key transmitted• OUT_SYNC

Participant is not in sync with the system id and key transmitted

Configurable False

system-id *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string* **lag members name** *reference* **system-id** *string*

Tree **system-id**

Description MAC address that defines the local system ID for the aggregate interface

Configurable False

timeout *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **interface name** *string* **lag members name** *reference* **timeout** *keyword*

Tree **timeout**

Description The timeout type (short or long) used by the participant

- Options
- LONG
Participant wishes to use long timeouts to detect status of the aggregate, i.e., will expect less frequent transmissions. Long timeout is 90 seconds.
 - SHORT
Participant wishes to use short timeouts, i.e., expects frequent transmissions to aggressively detect status changes. Short timeout is 3 seconds.

Configurable False

min-links *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> lag min-links <i>number</i>
Tree	min-links
Description	Specifies the minimum number of member interfaces that must be active for the aggregate interface to be available
Range	0 2 to 64
Configurable	True

last-change *string*

Context	interface name <i>string</i> last-change <i>string</i>
Tree	last-change
Description	The date and time of the most recent change to the interface state
Configurable	False

loopback-mode *boolean*

Context	interface name <i>string</i> loopback-mode <i>boolean</i>
Tree	loopback-mode
Description	When loopback-mode is set to true the port loops back packets that come in via the port
Configurable	True

mtu *number*

Context	interface name <i>string</i> mtu <i>number</i>
Tree	mtu
Description	Port MTU in bytes including ethernet overhead but excluding 4-bytes FCS If a packet exceeds this size it is dropped. Each linecard supports a maximum of 8 different port MTU values. The default value for a network port is taken from /system/mtu/default-port-mtu. The port MTU is not configurable for loopback and management ports.
Range	1500 to 9500
Units	bytes
Configurable	True

oper-down-reason *keyword*

Context	interface name <i>string</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Description	The first (and possibly only) reason for the port being operationally down
Options	<ul style="list-style-type: none">• port-admin-disabled• mda-admin-disabled• transceiver-admin-disabled• loopback• port-not-present• mda-not-present• transceiver-not-present• phy-initializing• lower-layer-down• mtu-resource-exceeded• unsupported-speed• invalid-transceiver-fec• other• fabric-availability
Configurable	False

oper-state *keyword*

Context	interface name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of the interface
Options	<ul style="list-style-type: none">• up• down
Configurable	False

qos

Context	interface name <i>string</i> qos
Tree	qos
Description	
Configurable	True

output

Context	interface name <i>string</i> qos output
Tree	output
Description	
Configurable	True

unicast-queue [queue-id](#) *number*

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i>
Tree	unicast-queue
Description	List of unicast queues
Configurable	True

[queue-id](#) *number*

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i>
Description	The queue identifier This has a one-to-one mapping to forwarding class.
Range	0 to 7
Configurable	True

queue-parameters

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-parameters
Tree	queue-parameters
Description	
Configurable	True

peak-rate-bps *number*

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-parameters peak-rate-bps <i>number</i>
Tree	peak-rate-bps
Description	The actual/operational peak rate in bits per second.
Configurable	False
Introduced	20.6.1

peak-rate-percent *number*

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-parameters peak-rate-percent <i>number</i>
Tree	peak-rate-percent
Description	The maximum percentage of port bandwidth that is available to the traffic in this unicast queue. The default is 100.
Range	0 to 100
Default	100
Configurable	True

strict-priority *boolean*

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-parameters strict-priority <i>boolean</i>
Tree	strict-priority
Description	When set to true the unicast queue is serviced as a strict priority queue, regardless of whether a weight is configured or its value. When set to false the unicast queue is serviced using WRR, even if the queue does not have a configured weight; in this case the default weight value of 1 is used. On 7220-D2 and 7220-D3 (Trident3 based) systems this setting also applies to the multicast queue for the same FC. To be more specific, the choice to use strict priority vs WRR applies to the scheduler node attached to the queue pair.
Default	true
Configurable	True

weight *number*

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-parameters weight <i>number</i>
Tree	weight
Description	Configures the relative weight of a round-robin queue. On 7220-D2 and 7220-D3 (Trident3 based) systems this setting also applies to the multicast queue for the same FC. To be more specific, the WRR weight applies to the scheduler node attached to the queue pair.
Range	1 to 255
Default	1
Configurable	True

queue-statistics

Context	interface name <i>string</i> queue-statistics
Tree	queue-statistics
Description	
Configurable	False

multicast-queue [queue-id](#) *number*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i>
Tree	multicast-queue
Description	List of multicast queues.
Configurable	False

queue-id *number*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i>
Description	The queue identifier This has a one-to-one mapping to forwarding class.
Range	0 to 7
Configurable	False

final-dropped-octets *number*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> final-dropped-octets <i>number</i>
Tree	final-dropped-octets
Description	Number of octets dropped by the multicast queue.
Default	0
Configurable	False

final-dropped-packets *number*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> final-dropped-packets <i>number</i>
Tree	final-dropped-packets
Description	Number of packets dropped by the multicast queue.
Default	0
Configurable	False

last-clear *string*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the statistics associated with this multicast queue were cleared
Configurable	False

transmitted-octets *number*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> transmitted-octets <i>number</i>
Tree	transmitted-octets
Description	Number of octets transmitted by the multicast queue.
Default	0
Configurable	False

transmitted-packets *number*

Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> transmitted-packets <i>number</i>
Tree	transmitted-packets
Description	Number of packets transmitted by the multicast queue.
Default	0
Configurable	False

unicast-queue *queue-id number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i>
Tree	unicast-queue
Description	List of unicast queues.
Configurable	False

queue-id *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i>
Description	The queue identifier This has a one-to-one mapping to forwarding class.
Range	0 to 7
Configurable	False

final-dropped-octets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> final-dropped-octets <i>number</i>
Tree	final-dropped-octets
Description	Number of octets in packets dropped by the egress queue itself.
Default	0
Configurable	False

final-dropped-packets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> final-dropped-packets <i>number</i>
Tree	final-dropped-packets
Description	Number of packets dropped by the unicast queue. On 7250-IXR (Jericho2-based) systems unicast packet drops related to egress port congestion should show up in the VOQ stats and not in this statistic.
Default	0
Configurable	False

last-clear *string*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the queue statistics were cleared
Configurable	False

transmitted-octets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> transmitted-octets <i>number</i>
Tree	transmitted-octets
Description	Number of octets transmitted by the unicast queue.
Default	0
Configurable	False

transmitted-packets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> transmitted-packets <i>number</i>
Tree	transmitted-packets
Description	Number of packets transmitted by the egress queue, including transit traffic and locally-originated traffic. This measures packets transmitted on the wire after drops in the VOQ queues, drops done by ACL entries and final drops by the EGQ itself (e.g. due to header compensation issues).
Default	0
Configurable	False

virtual-output-queue [slot](#) *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i>
Tree	virtual-output-queue
Description	List of virtual output queues that can send traffic to this egress queue. The list always has one entry for each IMM slot in the chassis, even if one or more slots are empty.
Configurable	False

slot *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i>
Description	The slot identifier for the virtual output queue.
Range	1 to 8
Configurable	False

dropped-octets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-octets <i>number</i>
Tree	dropped-octets
Description	The number of octets in packets dropped in the VOQ due to congestion at the egress port/queue.
Default	0
Configurable	False

dropped-packets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-packets <i>number</i>
Tree	dropped-packets
Description	The number of packets dropped in the VOQ due to congestion at the egress port/queue.
Default	0
Configurable	False

forwarded-octets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-octets <i>number</i>
Tree	forwarded-octets
Description	The number of octets in packets transmitted from the VOQ to the egress queue.
Default	0
Configurable	False

forwarded-packets *number*

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-packets <i>number</i>
Tree	forwarded-packets
Description	The number of packets transmitted from the VOQ to the egress queue. This reads 0 when the IMM associated with the VOQ is not inserted and it resets to 0 whenever the IMM associated with the VOQ is removed.
Default	0
Configurable	False

sflow

Context	interface name <i>string</i> sflow
Tree	sflow
Description	Context to configure sFlow parameters
Configurable	True

admin-state *keyword*

Context	interface name <i>string</i> sflow admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable sFlow on this interface
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

statistics

Context	interface name <i>string</i> statistics
Tree	statistics
Description	
Configurable	False

carrier-transitions *number*

Context	interface name <i>string</i> statistics carrier-transitions <i>number</i>
Tree	carrier-transitions
Description	Number of times the interface state has transitioned from down to up since the time the device restarted or the last clear.
Default	0
Configurable	False

in-broadcast-packets *number*

Context	interface name <i>string</i> statistics in-broadcast-packets <i>number</i>
Tree	in-broadcast-packets
Description	Corresponds to ifHCInBroadcastPkts from the IF-MIB.
Default	0
Configurable	False

in-error-packets *number*

Context	interface name <i>string</i> statistics in-error-packets <i>number</i>
Tree	in-error-packets
Description	Corresponds to ifInErrors from the IF-MIB.
Default	0
Configurable	False

in-fcs-error-packets *number*

Context	interface name <i>string</i> statistics in-fcs-error-packets <i>number</i>
Tree	in-fcs-error-packets
Description	Ingress FCS errors.
Default	0
Configurable	False

in-multicast-packets *number*

Context	interface name <i>string</i> statistics in-multicast-packets <i>number</i>
Tree	in-multicast-packets
Description	Corresponds to ifHCInMulticastPkts from the IF-MIB.
Default	0
Configurable	False

in-octets *number*

Context	interface name <i>string</i> statistics in-octets <i>number</i>
Tree	in-octets
Description	Corresponds to ifHCInOctets from the IFMIB.
Default	0
Configurable	False

in-unicast-packets *number*

Context	interface name <i>string</i> statistics in-unicast-packets <i>number</i>
Tree	in-unicast-packets
Description	Corresponds to ifHCInUcastPkts from the IF-MIB.
Default	0
Configurable	False

last-clear *string*

Context	interface name <i>string</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the interface counters were cleared.
Configurable	False

out-broadcast-packets *number*

Context	interface name <i>string</i> statistics out-broadcast-packets <i>number</i>
Tree	out-broadcast-packets
Description	Corresponds to ifHCOutBroadcastPkts from the IF-MIB.
Default	0
Configurable	False

out-error-packets *number*

Context	interface name <i>string</i> statistics out-error-packets <i>number</i>
Tree	out-error-packets
Description	Corresponds to ifOutErrors from the IF-MIB.
Default	0
Configurable	False

out-multicast-packets *number*

Context	interface name <i>string</i> statistics out-multicast-packets <i>number</i>
Tree	out-multicast-packets
Description	Corresponds to ifHCOutMulticastPkts from the IF-MIB.
Default	0
Configurable	False

out-octets *number*

Context	interface name <i>string</i> statistics out-octets <i>number</i>
Tree	out-octets
Description	Corresponds to ifHCOutOctets from the IF-MIB.
Default	0
Configurable	False

out-unicast-packets *number*

Context	interface name <i>string</i> statistics out-unicast-packets <i>number</i>
Tree	out-unicast-packets
Description	Corresponds to ifHCOutUcastPkts from the IF-MIB.
Default	0
Configurable	False

subinterface *index number*

Context	interface name <i>string</i> subinterface index <i>number</i>
Tree	subinterface
Description	The list of subinterfaces (logical interfaces) associated with a physical interface
Configurable	True
Max. Elements	4095

index *number*

Context	interface name <i>string</i> subinterface index <i>number</i>
Description	The index of the subinterface, or logical interface number
Range	0 to 9999
Configurable	True

acl

Context	interface name <i>string</i> subinterface index <i>number</i> acl
Tree	acl
Description	Container for ACL policies applied to the subinterface
Configurable	True

input

Context	interface name <i>string</i> subinterface index <i>number</i> acl input
Tree	input
Description	Container for ACL options that apply to ingress traffic on the subinterface
Configurable	True

ipv4-filter *reference*

Context	interface name <i>string</i> subinterface index <i>number</i> acl input ipv4-filter <i>reference</i>
Tree	ipv4-filter
Description	IPv4 ACL filter to be applied on this interface
Reference	acl ipv4-filter name <i>string</i>
Configurable	True

ipv6-filter *reference*

Context	interface name <i>string</i> subinterface index <i>number</i> acl input ipv6-filter <i>reference</i>
Tree	ipv6-filter
Description	IPv6 ACL filter to be applied on this interface
Reference	acl ipv6-filter name <i>string</i>
Configurable	True

output

Context	interface name <i>string</i> subinterface index <i>number</i> acl output
Tree	output
Description	Container for ACL options that apply to egress traffic on the subinterface
Configurable	True

ipv4-filter *reference*

Context	interface name <i>string</i> subinterface index <i>number</i> acl output ipv4-filter <i>reference</i>
Tree	ipv4-filter
Description	IPv4 ACL filter to be applied on this interface
Reference	acl ipv4-filter name <i>string</i>
Configurable	True

ipv6-filter *reference*

Context	interface name <i>string</i> subinterface index <i>number</i> acl output ipv6-filter <i>reference</i>
Tree	ipv6-filter
Description	IPv6 ACL filter to be applied on this interface
Reference	acl ipv6-filter name <i>string</i>
Configurable	True

admin-state *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> admin-state <i>keyword</i>
Tree	admin-state
Description	The configured, desired state of the interface
Default	enable
Options	<ul style="list-style-type: none">• enable

Configurable • disable
True

bridge-table



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context **interface name** *string* **subinterface index** *number* **bridge-table**
Tree **bridge-table**
Description Enable the Bridge Table on the subinterface and configure associated parameters
Configurable True

discard-unknown-src-mac *boolean*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context **interface name** *string* **subinterface index** *number* **bridge-table**
discard-unknown-src-mac *boolean*
Tree **discard-unknown-src-mac**
Description Discard frames with unknown source mac addresses
Default false
Configurable True

mac-duplication



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication
Tree	mac-duplication
Description	
Configurable	True

action *keyword*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication action <i>keyword</i>
Tree	action
Description	<p>Action to take on the subinterface upon detecting one or more mac addresses as duplicate on the subinterface. In particular:</p> <ul style="list-style-type: none"> • use-net-instance-action: upon detecting a duplicate mac on the subinterface, the action on the subinterface will be inherited from the action configured under <code>network-instance/bridge-table/mac-duplication/action</code>. • oper-down: if configured, upon detecting a duplicate mac on the subinterface, the subinterface will be brought oper-down. • blackhole: upon detecting a duplicate mac on the subinterface, the mac will be blackholed. Any frame received on this or any other subinterface with MAC SA matching a blackhole mac will be discarded. • stop-learning: upon detecting a duplicate mac on the subinterface, macs will no longer be learned on this subinterface.
Default	use-net-instance-action
Options	<ul style="list-style-type: none"> • use-net-instance-action • stop-learning • blackhole • oper-down
Configurable	True

mac-learning



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning
Tree	mac-learning
Description	
Configurable	True

admin-state *keyword*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning admin-state <i>keyword</i>
Tree	admin-state
Description	Configurable state of the learning procedures for dynamic mac addresses. If disabled, no mac addresses will be learned.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

aging



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning aging
Tree	aging
Description	
Configurable	True

admin-state *keyword*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning aging admin-state <i>keyword</i>
Tree	admin-state
Description	Configurable state of the aging for the dynamic mac entries in the bridge table. If disabled, dynamically learned mac entries will be programmed in the bridge table until the network instance is disabled.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

mac-limit



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-limit
Tree	mac-limit
Description	Bridge Table size and thresholds.
Configurable	True

maximum-entries *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context **interface name** *string* **subinterface index** *number* **bridge-table mac-limit maximum-entries** *number*

Tree **maximum-entries**

Description Maximum number of mac addresses allowed in the bridge-table.

Range 1 to 8192

Default 250

Configurable True

warning-threshold-pct *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context **interface name** *string* **subinterface index** *number* **bridge-table mac-limit warning-threshold-pct** *number*

Tree **warning-threshold-pct**

Description Percentage of the configured max-number-macs over which a warning is triggered. The warning message is cleared when the percentage drops below the configured percentage minus 5%

Range 6 to 100

Default 95

Configurable True

statistics



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics
Tree	statistics
Description	
Configurable	False

active-entries *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics active-entries <i>number</i>
Tree	active-entries
Description	The total number of entries that are active on the sub-interface.
Default	0
Configurable	False

mac-type **type** *keyword*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics mac-type type <i>keyword</i>
Tree	mac-type
Description	the type of the mac on the sub-interface.
Configurable	False

type *keyword*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics mac-type type <i>keyword</i>
Description	
Options	<ul style="list-style-type: none">• static• duplicate• learnt• irb-interface
Configurable	False

active-entries *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics mac-type type <i>keyword</i> active-entries <i>number</i>
Tree	active-entries
Description	The total number of entries of this type on the sub-interface
Default	0
Configurable	False

total-entries *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics mac-type type <i>keyword total-entries number</i>
Tree	total-entries
Description	The total number of macs of this type , active and inactive, on the sub-interface.
Default	0
Configurable	False

total-entries *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table statistics total-entries <i>number</i>
Tree	total-entries
Description	The total number of macs, active and inactive, on the sub-interface.
Default	0
Configurable	False

description *string*

Context	interface name <i>string</i> subinterface index <i>number</i> description <i>string</i>
Tree	description
Description	A user-configured description of the interface
String Length	1 to 255
Configurable	True

ip-mtu *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ip-mtu <i>number</i>
Tree	ip-mtu
Description	IP MTU of the subinterface in bytes, including the IP header but excluding Ethernet encapsulation IP MTU specifies the maximum sized IPv4 or IPv6 packet that can be transmitted on the subinterface. If an IPv4 or IPv6 packet exceeds this size it is dropped and this may result in the generation of an ICMP error message back to the source.

Each linecard supports a maximum of 4 different IP MTU values. The default value for a subinterface is taken from /system/mtu/default-ip-mtu. The IP MTU is not configurable for subinterfaces of loopback and management ports.

Range	1280 to 9486
Units	bytes
Configurable	True

ipv4

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4
Tree	ipv4
Description	Enable IPv4 on the subinterface and configure associated parameters When this is present in the running configuration, and even before an IPv4 address is configured, the subinterface starts to accept incoming packets with dest-ip 255.255.255.255, which is necessary to support dhcp-client functionality.
Configurable	True

address **ip-prefix** *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i>
Tree	address
Description	The list of IPv4 addresses assigned to the subinterface.
Configurable	True
Max. Elements	1

ip-prefix *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i>
Description	The IPv4 address and prefix length in CIDR notation
Configurable	True

origin *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> origin <i>keyword</i>
Tree	origin
Description	The origin of the IPv4 address.
Options	<ul style="list-style-type: none"> • other

	<ul style="list-style-type: none">• static• dhcp• link-layer• random
Configurable	False

status *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> status <i>keyword</i>
Tree	status
Description	The status of an IPv4 address
Options	<ul style="list-style-type: none">• preferred• inaccessible• tentative• duplicate
Configurable	False

vrrp

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp
Tree	vrrp
Description	VRRP Configuration and State under a IPv4 context of a sub-interface
Configurable	True

vrrp-group **virtual-router-id** *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i>
Tree	vrrp-group
Description	VRRP Group Specific Configuration under IPv4 context
Configurable	True

virtual-router-id *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i>
Description	VRRP Group Index
Configurable	True

accept-mode *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> accept-mode <i>boolean</i>
Tree	accept-mode
Description	Allows ssh,ping,traceroute to be accepted on the virtual IP address
Configurable	True

advertise-interval *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> advertise-interval <i>number</i>
Tree	advertise-interval
Description	The interval between VRRP messages
Configurable	True

authentication

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> authentication
Tree	authentication
Description	Context to configure authentication parameters
Configurable	True

text-key *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> authentication text-key <i>string</i>
Tree	text-key
Description	Configures the text string for cleartext or MD5 or hash key for MD5 hash.
Configurable	True

type *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> authentication type <i>keyword</i>
Tree	type
Description	Configures whether cleartext or md5 authentication is to be used for VRRP packets.
Options	<ul style="list-style-type: none">• text

- md5
 - md5-hash
- Configurable True

init-delay *number*

- Context **interface name** *string* **subinterface index** *number* **ipv4 address ip-prefix** *string* **vrrp vrrp-group virtual-router-id** *number* **init-delay** *number*
- Tree **init-delay**
- Description Initialization delay before a router that just rebooted will preempt an existing master router. Only applicable if preempt is enabled
- Configurable True

interface-tracking

- Context **interface name** *string* **subinterface index** *number* **ipv4 address ip-prefix** *string* **vrrp vrrp-group virtual-router-id** *number* **interface-tracking**
- Tree **interface-tracking**
- Description Interface reference for interface tracking
- Configurable True

priority-decrement *number*

- Context **interface name** *string* **subinterface index** *number* **ipv4 address ip-prefix** *string* **vrrp vrrp-group virtual-router-id** *number* **interface-tracking priority-decrement** *number*
- Tree **priority-decrement**
- Description For each tracked interface that is down then the priority is decremented by the specific amount to a minimum value of 0
- Configurable True

track-interface *reference*

- Context **interface name** *string* **subinterface index** *number* **ipv4 address ip-prefix** *string* **vrrp vrrp-group virtual-router-id** *number* **interface-tracking track-interface** *reference*
- Tree **track-interface**
- Description Interface reference for interface tracking. VRRP Group can track multiple interfaces.
- Reference **interface name** *string*
- Configurable True

preempt *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> preempt <i>boolean</i>
Tree	preempt
Description	Enable VRRP master pre-emption. If enabled, router with higher priority can assume master role. If disabled, router can only become master if no other master is present
Configurable	True

preempt-delay *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> preempt-delay <i>number</i>
Tree	preempt-delay
Description	Delay before a router preemts an existing master router, only applicable if preempt is enabled
Configurable	True

priority *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> priority <i>number</i>
Tree	priority
Description	Base VRRP Priority for associated Virtual Address
Configurable	True

state

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> state
Tree	state
Description	VRRP Per Group State
Configurable	True

operational-priority *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> state operational-priority <i>number</i>
Tree	operational-priority
Description	Reports the current VRRP operational priority.
Configurable	False

version *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> version <i>number</i>
Tree	version
Description	VRRP version for the Instance
Configurable	True

virtual-address (*ipv4-address | ipv6-address*)

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> virtual-address (<i>ipv4-address ipv6-address</i>)
Tree	virtual-address
Description	Associated Virtual IP address.
Configurable	True

allow-directed-broadcast *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 allow-directed-broadcast <i>boolean</i>
Tree	allow-directed-broadcast
Description	<p>When this is set to true the software is allowed to re-broadcast targeted broadcast IPv4 packets on this subinterface</p> <p>Detailed handling of subnet broadcast is as follows:</p> <p>If a targeted broadcast packet is received on subinterface X that has the matching subnet then it is delivered to the CPM and CPM will reply to an ICMP echo.</p> <p>If a targeted broadcast packet is received on subinterface X but the matching subnet is associated with subinterface Y, and subinterface Y is configured with <code>allow-directed-broadcasts=false</code> then it is delivered to the CPM and CPM replies to an ICMP echo per above, but it does not re-broadcast the packet on subinterface Y.</p> <p>If a targeted broadcast packet is received on subinterface X but the matching subnet is associated with subinterface Y, and subinterface Y is configured with <code>allow-directed-broadcasts=true</code> then it is delivered to the CPM and CPM replies to an ICMP echo per above, and CPM also re-broadcasts the packet on subinterface Y.</p>
Default	false
Configurable	True

arp

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp
Tree	arp
Description	
Configurable	True

neighbor [ipv4-address](#) *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>
Tree	neighbor
Description	List of static and dynamic ARP cache entries that map an IPv4 address to a MAC address To configure a static ARP entry a value must be written into this leaf and the link-layer-address leaf.
Configurable	True

[ipv4-address](#) *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>
Description	IPv4 address resolved by the ARP entry To configure a static neighbor entry a value must be written into this leaf and the link-layer-address leaf.
Configurable	True

expiration-time *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> expiration-time <i>string</i>
Tree	expiration-time
Description	The date and time when the dynamic ARP entry is set to expire
Configurable	False

link-layer-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> link-layer-address <i>string</i>
Tree	link-layer-address
Description	The resolving MAC address of the ARP entry

To configure a static ARP entry a value must be written into this leaf and the ipv4-address leaf.

Configurable True

origin *keyword*

Context **interface name** *string* **subinterface index** *number* **ipv4 arp neighbor ipv4-address** *string* **origin** *keyword*

Tree **origin**

Description The origin of the ARP entry

Options

- other
- static
- dynamic

Configurable False

timeout *number*

Context **interface name** *string* **subinterface index** *number* **ipv4 arp timeout** *number*

Tree **timeout**

Description Duration of time that dynamic ARP entries remain in the ARP cache before they expire
A change to this value does not affect existing entries until they are refreshed.

Range 60 to 65535

Default 14400

Units seconds

Configurable True

dhcp-client

Context **interface name** *string* **subinterface index** *number* **ipv4 dhcp-client**

Tree **dhcp-client**

Description Container for options related to DHCP

Configurable True

trace-options

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-client trace-options
Tree	trace-options
Description	Container for tracing DHCPv4 operations on the subinterface
Configurable	True

trace keyword

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-client trace-options trace keyword
Tree	trace
Description	List of events to trace
Options	<ul style="list-style-type: none">• messages Capture all DHCPv4 messages sent and received by the subinterface
Configurable	True

dhcp-relay

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay
Tree	dhcp-relay
Description	Container for options related to DHCPv4 relay
Configurable	True

option keyword

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay option keyword
Tree	option
Description	List of option82 suboptions to insert into relayed packet towards DHCPv4 server
Options	<ul style="list-style-type: none">• circuit-id Enable option 82 suboption 1 circuit-id into relayed packet towards DHCPv4 server, format=system_name/VRF_instance/sub-interface_id:vlan_id• remote-id Enable option 82 suboption 2 remote-id into relayed packet towards DHCPv4 server, format=client MAC address
Configurable	True

server (*ipv4-address | domain-name*)

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay server (<i>ipv4-address domain-name</i>)
Tree	server
Description	List of the DHCPv4 servers that the DHCPv4 relay function will relay DHCPv4 packets to/from
String Length	1 to 253
Configurable	True
Max. Elements	8
Min. Elements	1

source-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay source-address <i>string</i>
Tree	source-address
Description	Source IPv4 address of the relayed packets towards DHCPv4 servers this address must be a local IPv4 address configured on sub-interface where DHCPv4 relay is enabled and must be used as gi-address
Configurable	True

trace-options

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay trace-options
Tree	trace-options
Description	Container for tracing DHCPv4 relay operations on the subinterface
Configurable	True

trace *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay trace-options trace <i>keyword</i>
Tree	trace
Description	List of events to trace
Options	<ul style="list-style-type: none">• messages Capture all DHCPv4 messages sent and received by the subinterface
Configurable	True

ipv6

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6
Tree	ipv6
Description	<p>Enable IPv6 on the subinterface and configure associated parameters</p> <p>When this is present in the running configuration, and even before a global unicast IPv6 address is configured, chassis manager assigns an IPv6 link-local address to the subinterface, which will appear as a read-only entry in the address list. At this stage, the subinterface can receive IPv6 packets with any of the following destinations:</p> <ul style="list-style-type: none"> • IPv6 link-local address • solicited-node multicast address for the link-local address • ff02::1 (all IPv6 devices) • ff02::2 (all IPv6 routers)
Configurable	True

address **ip-prefix** *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i>
Tree	address
Description	The list of IPv6 addresses assigned to the subinterface.
Configurable	True
Max. Elements	2

ip-prefix *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i>
Description	<p>The IPv6 address and prefix-length in CIDR notation</p> <p>Only one IPv6 address is configurable per subinterface and it must be a valid global unicast address.</p>
Configurable	True

origin *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> origin <i>keyword</i>
Tree	origin
Description	The origin of the IPv6 address
Options	<ul style="list-style-type: none"> • other • static

- dhcp
 - link-layer
 - random
- Configurable False

status *keyword*

- Context **interface name** *string* **subinterface index** *number* **ipv6 address ip-prefix** *string* **status** *keyword*
- Tree **status**
- Description The status of an IPv6 address
- Options
- preferred
 - deprecated
 - invalid
 - inaccessible
 - unknown
 - tentative
 - duplicate
 - optimistic
- Configurable False

vrrp

- Context **interface name** *string* **subinterface index** *number* **ipv6 address ip-prefix** *string* **vrrp**
- Tree **vrrp**
- Description VRRP Configuration and State under a IPv6 context of a sub-interface
- Configurable True

vrrp-group **virtual-router-id** *number*

- Context **interface name** *string* **subinterface index** *number* **ipv6 address ip-prefix** *string* **vrrp** **vrrp-group virtual-router-id** *number*
- Tree **vrrp-group**
- Description VRRP Group Specific Configuration under IPv6 context
- Configurable True

virtual-router-id *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i>
Description	VRRP Group Index
Configurable	True

accept-mode *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> accept-mode <i>boolean</i>
Tree	accept-mode
Description	Allows ssh,ping,traceroute to be accepted on the virtual IP address
Configurable	True

advertise-interval *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> advertise-interval <i>number</i>
Tree	advertise-interval
Description	The interval between VRRP messages
Configurable	True

authentication

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> authentication
Tree	authentication
Description	Context to configure authentication parameters
Configurable	True

text-key *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> authentication text-key <i>string</i>
Tree	text-key
Description	Configures the text string for cleartext or MD5 or hash key for MD5 hash.
Configurable	True

type *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> authentication type <i>keyword</i>
Tree	type
Description	Configures whether cleartext or md5 authentication is to be used for VRRP packets.
Options	<ul style="list-style-type: none">• text• md5• md5-hash
Configurable	True

init-delay *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> init-delay <i>number</i>
Tree	init-delay
Description	Initialization delay before a router that just rebooted will preempt an existing master router. Only applicable if preempt is enabled
Configurable	True

interface-tracking

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> interface-tracking
Tree	interface-tracking
Description	Interface reference for interface tracking
Configurable	True

priority-decrement *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> interface-tracking priority-decrement <i>number</i>
Tree	priority-decrement
Description	For each tracked interface that is down then the priority is decremented by the specific amount to a minimum value of 0
Configurable	True

track-interface *reference*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> interface-tracking track-interface <i>reference</i>
Tree	track-interface
Description	Interface reference for interface tracking. VRRP Group can track multiple interfaces.
Reference	interface name <i>string</i>
Configurable	True

preempt *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> preempt <i>boolean</i>
Tree	preempt
Description	Enable VRRP master pre-emption. If enabled, router with higher priority can assume master role. If disabled, router can only become master if no other master is present
Configurable	True

preempt-delay *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> preempt-delay <i>number</i>
Tree	preempt-delay
Description	Delay before a router preemts an existing master router, only applicable if preempt is enabled
Configurable	True

priority *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> priority <i>number</i>
Tree	priority
Description	Base VRRP Priority for associated Virtual Address
Configurable	True

state

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> state
Tree	state
Description	VRRP Per Group State
Configurable	True

operational-priority *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> state operational-priority <i>number</i>
Tree	operational-priority
Description	Reports the current VRRP operational priority.
Configurable	False

version *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> version <i>number</i>
Tree	version
Description	VRRP version for the Instance
Configurable	True

virtual-address (*ipv4-address | ipv6-address*)

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> vrrp vrrp-group virtual-router-id <i>number</i> virtual-address (<i>ipv4-address ipv6-address</i>)
Tree	virtual-address
Description	Associated Virtual IP address.
Configurable	True

dhcp-client

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-client
Tree	dhcp-client
Description	Container for options related to DHCPv6
Configurable	True

trace-options

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-client trace-options
Tree	trace-options
Description	Container for tracing DHCPv6 operations on the subinterface
Configurable	True

trace *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-client trace-options trace keyword
Tree	trace
Description	List of events to trace
Options	<ul style="list-style-type: none">• <code>messages</code> Capture all DHCPv6 messages sent and received by the subinterface
Configurable	True

dhcp-relay

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay
Tree	dhcp-relay
Description	Container for options related to DHCPv6 relay
Configurable	True

option *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay option keyword
Tree	option
Description	List of options to insert into relayed packet towards DHCPv6 server
Options	<ul style="list-style-type: none">• <code>interface-id</code> Enable option 18 Interface-Id into relayed packet towards DHCPv6 server, format=<code>system_name/VRF_instance/sub-interface_id:vlan_id</code>• <code>remote-id</code> Enable option 37 Remote Identifier into relayed packet towards DHCPv6 server, format=<code>client MAC address</code>
Configurable	True

server (*ipv6-address | domain-name*)

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay server (<i>ipv6-address domain-name</i>)
Tree	server
Description	List of the DHCPv6 servers that the DHCPv6 relay function will relay DHCPv6 packets to/from
String Length	1 to 253
Configurable	True
Max. Elements	8
Min. Elements	1

source-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay source-address <i>string</i>
Tree	source-address
Description	Source IPv6 address of the relayed packets towards DHCPv6 servers this address must be a local IPv6 address configured on sub-interface where DHCPv6 relay is enabled
Configurable	True

trace-options

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay trace-options
Tree	trace-options
Description	Container for tracing DHCPv6 relay operations on the subinterface
Configurable	True

trace *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay trace-options trace <i>keyword</i>
Tree	trace
Description	List of events to trace
Options	<ul style="list-style-type: none">• messages Capture all DHCPv6 messages sent and received by the subinterface
Configurable	True

neighbor-discovery

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery
Tree	neighbor-discovery
Description	
Configurable	True

duplicate-address-detection *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery duplicate-address-detection <i>boolean</i>
Tree	duplicate-address-detection
Description	Enables Duplicate Address Detection on all tentative addresses This applies to link-local and global unicast addresses. Only one transmission is done; there are no retransmissions.
Default	true
Configurable	True

neighbor [ipv6-address](#) *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Tree	neighbor
Description	List of static and dynamic ND cache entries that map an IPv6 address to a MAC address
Configurable	True

ipv6-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Description	IPv6 address resolved by the ND cache entry To configure a static neighbor entry a value must be written into this leaf and the link-layer-address leaf.
Configurable	True

current-state *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> current-state <i>keyword</i>
Tree	current-state
Description	The Neighbor Unreachability Detection state
Options	<ul style="list-style-type: none">• incomplete• reachable• stale• delay• probe
Configurable	False

is-router *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> is-router <i>boolean</i>
Tree	is-router
Description	Indicates that the neighbor node claims to be a router (R bit in the Neighbor Advertisement message)
Configurable	False

link-layer-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> link-layer-address <i>string</i>
Tree	link-layer-address
Description	The resolving MAC address of the ND cache entry To configure a static neighbor entry a value must be written into this leaf and the ipv6-address leaf.
Configurable	True

next-state-time *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> next-state-time <i>string</i>
Tree	next-state-time
Description	The date and time when the neighbor state is expected to transition to the next state
Configurable	False

origin *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> origin <i>keyword</i>
Tree	origin
Description	The origin of the neighbor cache entry.
Options	<ul style="list-style-type: none">• other• static• dynamic
Configurable	False

reachable-time *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery reachable-time <i>number</i>
Tree	reachable-time
Description	The period of time that a dynamic IPv6 neighbor cache entry is considered reachable after a reachability confirmation event After this time expires the neighbor state moves to STALE.
Range	30 to 3600
Default	30
Units	seconds
Configurable	True

stale-time *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery stale-time <i>number</i>
Tree	stale-time
Description	The maximum time that a dynamic IPv6 neighbor cache entry can remain in the STALE state before it is removed This limit is reached only if no traffic is sent/queued towards the neighbor during the entire duration of the timer.
Range	60 to 65535
Default	14400
Units	seconds
Configurable	True

router-advertisement

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement
Tree	router-advertisement
Description	Container for configuring IPv6 router discovery options
Configurable	True

router-role

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role
Tree	router-role
Description	IPv6 router advertisement options that apply when the role of the interface is a router interface.
Configurable	True

admin-state *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the sending of router advertisements on the subinterface.
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

current-hop-limit *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role current-hop-limit <i>number</i>
Tree	current-hop-limit
Description	The current hop limit to advertise in the router advertisement messages.
Default	64
Configurable	True

ip-mtu *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role ip-mtu <i>number</i>
Tree	ip-mtu
Description	The IP MTU to advertise in the router advertisement messages and that hosts should associate with the link on which these messages are received.
Range	1280 to 9486
Configurable	True

managed-configuration-flag *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role managed-configuration-flag <i>boolean</i>
Tree	managed-configuration-flag
Description	When this is set the M-bit is set in the router advertisement messages, indicating that hosts should use DHCPv6 to obtain IPv6 addresses.
Default	false
Configurable	True

max-advertisement-interval *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role max-advertisement-interval <i>number</i>
Tree	max-advertisement-interval
Description	<p>The maximum time between sending router advertisement messages to the all-nodes multicast address.</p> <p>Each subinterface has its own timer. Whenever the timer fires the message is sent and then the timer is reset to a uniformly distributed random value between min-advertisement-interval and max-advertisement-interval. The RA message can be sent before timer expiry in response to a RS message.</p>
Range	4 to 1800
Default	600
Units	seconds
Configurable	True

min-advertisement-interval *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role min-advertisement-interval <i>number</i>
Tree	min-advertisement-interval
Description	The minimum time between sending router advertisement messages to the all-nodes multicast address. Each subinterface has its own timer. Whenever the timer fires the message is sent and then the timer is reset to a uniformly distributed random value between min-advertisement-interval and max-advertisement-interval. The RA message can be sent before timer expiry in response to a RS message.
Range	3 to 1350
Default	200
Units	seconds
Configurable	True

other-configuration-flag *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role other-configuration-flag <i>boolean</i>
Tree	other-configuration-flag
Description	When this is set the O-bit is set in the router advertisement messages, indicating that hosts should use DHCPv6 to obtain other configuration information (besides addresses).
Default	false
Configurable	True

prefix **ipv6-prefix** *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i>
Tree	prefix
Description	The list of IPv6 prefixes to advertise in the router advertisement messages.
Configurable	True
Max. Elements	1

ipv6-prefix *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i>
Description	An IPv6 global unicast address prefix.
Configurable	True

autonomous-flag *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i> autonomous-flag <i>boolean</i>
Tree	autonomous-flag
Description	When this is set in the prefix information option hosts can use the prefix for stateless address autoconfiguration (SLAAC).
Default	false
Configurable	True

on-link-flag *boolean*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i> on-link-flag <i>boolean</i>
Tree	on-link-flag
Description	When this is set in the prefix information option hosts can use the prefix for on-link determination.
Default	false
Configurable	True

preferred-lifetime (*keyword | number*)

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i> preferred-lifetime (<i>keyword number</i>)
Tree	preferred-lifetime
Description	The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.
Default	604800
Units	seconds
Options	<ul style="list-style-type: none">infinite
Configurable	True

valid-lifetime (*keyword | number*)

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i> valid-lifetime (<i>keyword number</i>)
Tree	valid-lifetime
Description	The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination.
Default	2592000
Units	seconds
Options	<ul style="list-style-type: none">infinite
Configurable	True

reachable-time *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role reachable-time <i>number</i>
Tree	reachable-time
Description	The time, in milliseconds, that is advertised as the reachable time in RA messages and that hosts use for the ICMPv6 Neighbor Unreachability Detection algorithm. A value of zero means unspecified by this router.
Range	0 to 3600000
Default	0
Configurable	True

retransmit-time *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role retransmit-time <i>number</i>
Tree	retransmit-time
Description	The time, in milliseconds, that is advertised as the retrans-timer in RA messages and that hosts use for address resolution and the Neighbor Unreachability Detection algorithm. It represents the time between retransmitted NS messages. A value of zero means unspecified by this router.
Range	0 to 1800000
Default	0
Configurable	True

router-lifetime *number*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role router-lifetime <i>number</i>
Tree	router-lifetime
Description	The lifetime in seconds that is advertised as the router lifetime in RA messages. This indicates the time period for which the advertising router can be used as a default router/gateway. A value of 0 means the router should not be used as a default gateway.
Range	0 to 9000
Default	1800
Configurable	True

trace-options

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement trace-options
Tree	trace-options
Description	Container for tracing Router Solicitation and Router Advertisement messages on the subinterface
Configurable	True

trace *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement trace-options trace <i>keyword</i>
Tree	trace
Description	List of events to trace
Options	<ul style="list-style-type: none"> messages Capture all router-solicitation and router-advertisement messages sent and received by the subinterface
Configurable	True

I2-mtu *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	interface name <i>string</i> subinterface index <i>number</i> l2-mtu <i>number</i>
Tree	l2-mtu
Description	<p>Layer-2 MTU of the subinterface in bytes, including the Ethernet header and VLAN tags, and excluding 4-bytes FCS.</p> <p>L2 MTU specifies the maximum sized Ethernet frame that can be transmitted on the subinterface. If a frame exceeds this size it is discarded. If the l2-mtu of the subinterface exceeds the port-mtu of the associated interface, the subinterface will remain operationally down.</p> <p>The default value for a subinterface is taken from /system/mtu/default-l2-mtu. The L2 MTU is only configurable for bridged subinterfaces.</p>
Range	1500 to 9500
Units	bytes
Configurable	True

last-change *string*

Context	interface name <i>string</i> subinterface index <i>number</i> last-change <i>string</i>
Tree	last-change
Description	The date and time of the most recent change to the subinterface state
Configurable	False

name *string*

Context	interface name <i>string</i> subinterface index <i>number</i> name <i>string</i>
Tree	name
Description	The system assigned name of the subinterface. It is formed by taking the base interface name and appending a dot (.) and the subinterface index number. For example, ethernet-2/1.0
Configurable	False

oper-down-reason *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Description	The first (and possibly only) reason for the subinterface being operationally down
Options	<ul style="list-style-type: none"> • admin-disabled • port-down • mtu-resource-exceeded • mtu-too-large

	<ul style="list-style-type: none">• no-ip-config• ip-mtu-larger-than-oper-mac-vrf-mtu• other
Configurable	False

oper-state *keyword*

Context	interface name <i>string</i> subinterface index <i>number</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of the subinterface
Options	<ul style="list-style-type: none">• up• down
Configurable	False

qos

Context	interface name <i>string</i> subinterface index <i>number</i> qos
Tree	qos
Description	
Configurable	True

input

Context	interface name <i>string</i> subinterface index <i>number</i> qos input
Tree	input
Description	
Configurable	True

classifiers

Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers
Tree	classifiers
Description	
Configurable	True

dscp reference



Note: This command is available for the following platforms:

- 7220 IXR-D3
- 7220 IXR-D2

Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers dscp <i>reference</i>
Tree	dscp
Description	Reference to the name of a DSCP classifier policy that applies to both IPv4 and IPv6 traffic.
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True

ipv4-dscp reference



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers ipv4-dscp <i>reference</i>
Tree	ipv4-dscp
Description	Reference to the name of a DSCP classifier policy that applies only to IPv4 traffic.
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True

ipv6-dscp reference



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers ipv6-dscp <i>reference</i>
Tree	ipv6-dscp
Description	Reference to the name of a DSCP classifier policy that applies only to IPv6 traffic.
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True

mpls-traffic-class *reference*

Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers mpls-traffic-class reference
Tree	mpls-traffic-class
Description	Reference to the name of an MPLS traffic-class classifier policy
Reference	qos classifiers mpls-traffic-class-policy name <i>string</i>
Configurable	True

output

Context	interface name <i>string</i> subinterface index <i>number</i> qos output
Tree	output
Description	
Configurable	True

rewrite-rules

Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules
Tree	rewrite-rules
Description	
Configurable	True

dscp *reference*



Note: This command is available for the following platforms:

- 7220 IXR-D3
- 7220 IXR-D2

Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules dscp reference
Tree	dscp
Description	Reference to the name of a DSCP rewrite-rule policy that applies to both IPv4 and IPv6 traffic.
Reference	qos rewrite-rules dscp-policy name <i>string</i>
Configurable	True

ipv4-dscp reference



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules ipv4-dscp <i>reference</i>
Tree	ipv4-dscp
Description	Reference to the name of a DSCP rewrite-rule policy that applies only to IPv4 traffic.
Reference	qos rewrite-rules dscp-policy name <i>string</i>
Configurable	True

ipv6-dscp reference



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules ipv6-dscp <i>reference</i>
Tree	ipv6-dscp
Description	Reference to the name of a DSCP rewrite-rule policy that applies only to IPv6 traffic.
Reference	qos rewrite-rules dscp-policy name <i>string</i>
Configurable	True

mpls-traffic-class reference

Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules mpls-traffic-class <i>reference</i>
Tree	mpls-traffic-class
Description	Reference to the name of an MPLS traffic-class rewrite-rule policy
Reference	qos rewrite-rules mpls-traffic-class-policy name <i>string</i>
Configurable	True

statistics

Context	interface name <i>string</i> subinterface index <i>number</i> statistics
Tree	statistics
Description	Container for subinterface statistics, counting IPv4 packets, IPv6 packets and MPLS packets in aggregate
Configurable	False

in-discarded-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-discarded-packets <i>number</i>
Tree	in-discarded-packets
Description	The total number of input IPv4+IPv6+MPLS packets (transit and terminating traffic) that were dropped for any of the following reasons: <ul style="list-style-type: none"> • ingress ACL drop action (applies to transit + terminating) • CPM filter drop action (applies to terminating only) • VOQ congestion discards (applies to terminating towards CPM and transit towards output port) • unicast destination MAC address is not the MAC address of the subinterface • packet matched a route with a blackhole next-hop • packet was non-terminating and its TTL expired • packet matched a route with a next-hop via another subinterface but the next-hop address was not resolvable by ARP/ND • packet is a host address on another subinterface but the host address was not resolvable by ARP/ND
Default	0
Configurable	False

in-error-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-error-packets <i>number</i>
Tree	in-error-packets
Description	The total number of input IPv4+IPv6+MPLS packets discarded due to errors, counting transit and terminating traffic The sum of the following RFC 4293 counters: ipIfStatsInHdrErrors ipIfStatsInNoRoutes ipIfStatsInAddrErrors ipIfStatsInUnknownProtos ipIfStatsInTruncatedPkts
Default	0
Configurable	False

in-forwarded-octets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-forwarded-octets <i>number</i>
Tree	in-forwarded-octets
Description	The number of octets received in input IPv4+IPv6+MPLS packets received on this subinterface and counted in in-forwarded-packets
Default	0
Configurable	False

in-forwarded-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-forwarded-packets <i>number</i>
Tree	in-forwarded-packets
Description	<p>The number of input IPv4+IPv6+MPLS packets received on this subinterface for which the router was not the final destination and for which the router attempted to find a route or label entry to forward them to that final destination</p> <p>Note that non-terminating IPv4 packets with options and non-terminating IPv6 packets with extension headers are included in this count (and not dropped) as are packets that trigger ICMP/ICMPv6 redirect messages.</p>
Default	0
Configurable	False

in-octets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-octets <i>number</i>
Tree	in-octets
Description	The total number of octets received in input IPv4+IPv6+MPLS packets, counting transit and terminating traffic
Default	0
Configurable	False

in-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-packets <i>number</i>
Tree	in-packets
Description	The total number of input IPv4+IPv6+MPLS packets received, counting transit and terminating traffic

	This equals the sum of: in-error-packets in-discarded-packets in-terminated-packets in-forwarded-packets
Default	0
Configurable	False

in-terminated-octets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-terminated-octets <i>number</i>
Tree	in-terminated-octets
Description	The total number of octets in input IPv4+IPv6+MPLS packets that were received on this subinterface and counted in in-terminated-packets
Default	0
Configurable	False

in-terminated-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-terminated-packets <i>number</i>
Tree	in-terminated-packets
Description	The total number of input IPv4+IPv6+MPLS packets that were received on this subinterface and that have a destination IP address matching a local interface address or an IPv6 multicast address to which the interface belongs. The count includes packets eventually discarded by the CPM. Such discards include: <ul style="list-style-type: none"> • packets with unsupported IP protocol numbers • packets destined to TCP/UDP ports that are not open/listening • IPv4 packets with any IP options • IPv6 packets with any extension headers
Default	0
Configurable	False

last-clear *string*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the subinterface counters were cleared.
Configurable	False

out-discarded-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-discarded-packets <i>number</i>
Tree	out-discarded-packets
Description	The total number of IPv4+IPv6+MPLS packets, originating and transit, sent towards this subinterface that were dropped. Always zero for now.
Default	0
Configurable	False

out-error-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-error-packets <i>number</i>
Tree	out-error-packets
Description	The number of IPv4+IPv6+MPLS packets, originating and transit, for which this router was successful in finding a path to their final destination through this subinterface but an error prevented their transmission Currently, the only expected reason for this is because the IPv4 or MPLS packet size exceeded the MTU and fragmentation was not allowed or not supported
Default	0
Configurable	False

out-forwarded-octets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-forwarded-octets <i>number</i>
Tree	out-forwarded-octets
Description	The number of octets in transit IPv4+IPv6+MPLS packets which the router attempted to route out this subinterface
Default	0
Configurable	False

out-forwarded-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-forwarded-packets <i>number</i>
Tree	out-forwarded-packets
Description	The number of transit IPv4+IPv6+MPLS packets which the router attempted to route out this subinterface
Default	0
Configurable	False

out-octets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-octets <i>number</i>
Tree	out-octets
Description	The total number of octets in IPv4+IPv6+MPLS packets delivered to the lower layers for transmission
Default	0
Configurable	False

out-originated-octets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-originated-octets <i>number</i>
Tree	out-originated-octets
Description	The number of octets in IPv4+IPv6+MPLS packets which originated on the CPM and which the router attempted to route out this subinterface
Default	0
Configurable	False

out-originated-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-originated-packets <i>number</i>
Tree	out-originated-packets
Description	The number of IPv4+IPv6+MPLS packets which originated on the CPM and which the router attempted to route out this subinterface This includes all originated ICMP/ICMPv6 messages.
Default	0
Configurable	False

out-packets *number*

Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-packets <i>number</i>
Tree	out-packets
Description	The total number of IPv4+IPv6+MPLS packets that this router supplied to the lower layers for transmission This includes packets generated locally and those forwarded by this router. If there are no queue drops it is equal to: <out-forwarded-packets> + <out-originated-packets> - <out-error-packets> - <out-discarded-packets>
Default	0
Configurable	False

type *identityref*

Context	interface name <i>string</i> subinterface index <i>number</i> type <i>identityref</i>
Tree	type
Description	The value of this leaf indicates the context in which the ethernet subinterface will be used in
Options	<ul style="list-style-type: none">• routed indicates subinterface is used in a routed context• bridged indicates subinterface is used in a bridged context
Configurable	True

vlan

Context	interface name <i>string</i> subinterface index <i>number</i> vlan
Tree	vlan
Description	Parameters for VLAN definition under SRL interfaces.
Configurable	True

encap

Context	interface name <i>string</i> subinterface index <i>number</i> vlan encap
Tree	encap
Description	VLAN match parameters for the associated subinterface.
Configurable	True

single-tagged

Context	interface name <i>string</i> subinterface index <i>number</i> vlan encap single-tagged
Tree	single-tagged
Description	Match single-tagged packets with a single VLAN identifier.
Configurable	True

vlan-id *number*

Context	interface name <i>string</i> subinterface index <i>number</i> vlan encap single-tagged vlan-id <i>number</i>
Tree	vlan-id
Description	VLAN identifier for single-tagged packets.
Range	1 to 4094
Configurable	True

traffic-rate

Context	interface name <i>string</i> traffic-rate
Tree	traffic-rate
Description	Container for traffic rate statistics
Configurable	False

in-bps *number*

Context	interface name <i>string</i> traffic-rate in-bps <i>number</i>
Tree	in-bps
Description	The ingress bandwidth utilization of the port, updated every 10 seconds
Configurable	False

out-bps *number*

Context	interface name <i>string</i> traffic-rate out-bps <i>number</i>
Tree	out-bps
Description	The egress bandwidth utilization of the port, updated every 10 seconds
Configurable	False

transceiver

Context	interface name <i>string</i> transceiver
Tree	transceiver
Description	
Configurable	True

admin-state *keyword*

Context	interface name <i>string</i> transceiver admin-state <i>keyword</i>
Tree	admin-state
Description	The configured, desired state of the transceiver
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

channel index *number*

Context	interface name <i>string</i> transceiver channel index <i>number</i>
Tree	channel
Description	List of physical channels supported by the transceiver that are associated with this particular port
Configurable	False

index *number*

Context	interface name <i>string</i> transceiver channel index <i>number</i>
Description	Index of the physical channel or lane
Range	1 to 10
Configurable	False

input-power

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power
Tree	input-power
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the Rx power is above the high-alarm-threshold and set to false whenever the Rx power is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the Rx power is above the high-warning-threshold and set to false whenever the Rx power is below the high-warning-threshold
Configurable	False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current value of the optical Rx power in dBm
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the Rx power is below the low-alarm-threshold and set to false whenever the Rx power is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the Rx power is below the low-warning-threshold and set to false whenever the Rx power is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

laser-bias-current

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current
Tree	laser-bias-current
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the laser bias current is above the high-alarm-threshold and set to false whenever the laser bias current is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the laser bias current is above the high-warning-threshold and set to false whenever the laser bias current is below the high-warning-threshold
Configurable	False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current value of the laser bias current in mA
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the laser bias current is below the low-alarm-threshold and set to false whenever the laser bias current is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the laser bias current is below the low-warning-threshold and set to false whenever the laser bias current is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

output-power

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power
Tree	output-power
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the Tx power is above the high-alarm-threshold and set to false whenever the Tx power is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the Tx power is above the high-warning-threshold and set to false whenever the Tx power is below the high-warning-threshold
Configurable	False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current value of the optical Tx power in dBm
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the Tx power is below the low-alarm-threshold and set to false whenever the Tx power is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the Tx power is below the low-warning-threshold and set to false whenever the Tx power is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

wavelength *decimal-number*

Context	interface name <i>string</i> transceiver channel index <i>number</i> wavelength <i>decimal-number</i>
Tree	wavelength
Description	Wavelength of the transmitting laser in nanometers
Configurable	False

connector-type *keyword*

Context	interface name <i>string</i> transceiver connector-type <i>keyword</i>
Tree	connector-type
Description	Specifies the fiber connector type of the transceiver associated with the port.
Options	<ul style="list-style-type: none">• SC• LC

	<ul style="list-style-type: none">• MPO-1x12• no-separable-connector• unknown
Configurable	False

date-code *string*

Context	interface name <i>string</i> transceiver date-code <i>string</i>
Tree	date-code
Description	Transceiver date code.
Configurable	False

ddm-events *boolean*

Context	interface name <i>string</i> transceiver ddm-events <i>boolean</i>
Tree	ddm-events
Description	When set to true, log events and state related to the Digital Diagnostic Monitoring (DDM) capabilities of the transceiver are generated and populated. When set to false, no DDM-related log events and state are generated and populated for this port/transceiver. Default is false (for interfaces that support transceivers).
Configurable	True

ethernet-pmd *string*

Context	interface name <i>string</i> transceiver ethernet-pmd <i>string</i>
Tree	ethernet-pmd
Description	Specifies the Ethernet compliance code of the transceiver associated with the port.
Configurable	False

fault-condition *boolean*

Context	interface name <i>string</i> transceiver fault-condition <i>boolean</i>
Tree	fault-condition
Description	Indicates if a fault condition exists in the transceiver.
Configurable	False

form-factor *keyword*

Context	interface name <i>string</i> transceiver form-factor <i>keyword</i>
Tree	form-factor
Description	Specifies the transceiver form factor associated with the port.
Options	<ul style="list-style-type: none">• CFP2• CFP2-ACO• CFP4• QSFP• QSFPplus• QSFP28• QSFPDD• SFP• SFPplus• Non-pluggable• Other• SFP28
Configurable	False

forward-error-correction *keyword*

Context	interface name <i>string</i> transceiver forward-error-correction <i>keyword</i>
Tree	forward-error-correction
Description	The forward error correction algorithm to use on the optical channel 100G interfaces support disabled and rs-528 as valid options that do not bring the port down. 400G interfaces support rs-544 as the only valid option that does not bring the port down.
Options	<ul style="list-style-type: none">• disabled• rs-528• rs-544
Configurable	True

input-power

Context	interface name <i>string</i> transceiver input-power
Tree	input-power
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver input-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the Rx power is above the high-alarm-threshold and set to false whenever the Rx power is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver input-power high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver input-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the Rx power is above the high-warning-threshold and set to false whenever the Rx power is below the high-warning-threshold
Configurable	False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver input-power high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver input-power latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current value of the optical Rx power in dBm
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver input-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the Rx power is below the low-alarm-threshold and set to false whenever the Rx power is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver input-power low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver input-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the Rx power is below the low-warning-threshold and set to false whenever the Rx power is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver input-power low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

laser-bias-current

Context	interface name <i>string</i> transceiver laser-bias-current
Tree	laser-bias-current
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver laser-bias-current high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the laser bias current is above the high-alarm-threshold and set to false whenever the laser bias current is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver laser-bias-current high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver laser-bias-current high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the laser bias current is above the high-warning-threshold and set to false whenever the laser bias current is below the high-warning-threshold
Configurable	False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver laser-bias-current high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver laser-bias-current latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current value of the laser bias current in mA
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver laser-bias-current low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the laser bias current is below the low-alarm-threshold and set to false whenever the laser bias current is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver laser-bias-current low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver laser-bias-current low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the laser bias current is below the low-warning-threshold and set to false whenever the laser bias current is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver laser-bias-current low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

oper-state *keyword*

Context	interface name <i>string</i> transceiver oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of the transceiver
Options	<ul style="list-style-type: none">• up• down

Configurable • not-present
False

output-power

Context [interface name](#) *string* [transceiver](#) [output-power](#)
Tree [output-power](#)
Description
Configurable False

high-alarm-condition *boolean*

Context [interface name](#) *string* [transceiver](#) [output-power](#) [high-alarm-condition](#) *boolean*
Tree [high-alarm-condition](#)
Description Set to true whenever the Tx power is above the high-alarm-threshold and set to false
 whenever the Tx power is below the high-alarm-threshold
Configurable False

high-alarm-threshold *decimal-number*

Context [interface name](#) *string* [transceiver](#) [output-power](#) [high-alarm-threshold](#) *decimal-number*
Tree [high-alarm-threshold](#)
Description Read from the installed transceiver
Configurable False

high-warning-condition *boolean*

Context [interface name](#) *string* [transceiver](#) [output-power](#) [high-warning-condition](#) *boolean*
Tree [high-warning-condition](#)
Description Set to true whenever the Tx power is above the high-warning-threshold and set to false
 whenever the Tx power is below the high-warning-threshold
Configurable False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver output-power high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver output-power latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current value of the optical Tx power in dBm
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver output-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the Tx power is below the low-alarm-threshold and set to false whenever the Tx power is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver output-power low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver output-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the Tx power is below the low-warning-threshold and set to false whenever the Tx power is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver output-power low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

serial-number *string*

Context	interface name <i>string</i> transceiver serial-number <i>string</i>
Tree	serial-number
Description	Transceiver serial number.
Configurable	False

temperature

Context	interface name <i>string</i> transceiver temperature
Tree	temperature
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver temperature high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the temperature is above the high-alarm-threshold and set to false whenever the temperature is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *number*

Context	interface name <i>string</i> transceiver temperature high-alarm-threshold <i>number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver temperature high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the temperature is above the high-warning-threshold and set to false whenever the temperature is below the high-warning-threshold
Configurable	False

high-warning-threshold *number*

Context	interface name <i>string</i> transceiver temperature high-warning-threshold <i>number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *number*

Context	interface name <i>string</i> transceiver temperature latest-value <i>number</i>
Tree	latest-value
Description	The current temperature of the transceiver module in degrees Celsius
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver temperature low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the temperature is below the low-alarm-threshold and set to false whenever the temperature is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *number*

Context	interface name <i>string</i> transceiver temperature low-alarm-threshold <i>number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver temperature low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the temperature is below the low-warning-threshold and set to false whenever the temperature is above the low-warning-threshold
Configurable	False

low-warning-threshold *number*

Context	interface name <i>string</i> transceiver temperature low-warning-threshold <i>number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

vendor *string*

Context	interface name <i>string</i> transceiver vendor <i>string</i>
Tree	vendor
Description	Name of the transceiver vendor.
Configurable	False

vendor-part-number *string*

Context	interface name <i>string</i> transceiver vendor-part-number <i>string</i>
Tree	vendor-part-number
Description	Vendor's part number for the transceiver.
Configurable	False

vendor-revision *string*

Context	interface name <i>string</i> transceiver vendor-revision <i>string</i>
Tree	vendor-revision
Description	Vendor's revision number for the transceiver.
Configurable	False

voltage

Context	interface name <i>string</i> transceiver voltage
Tree	voltage
Description	
Configurable	False

high-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver voltage high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Description	Set to true whenever the module voltage is above the high-alarm-threshold and set to false whenever the module voltage is below the high-alarm-threshold
Configurable	False

high-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver voltage high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

high-warning-condition *boolean*

Context	interface name <i>string</i> transceiver voltage high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Description	Set to true whenever the module voltage is above the high-warning-threshold and set to false whenever the module voltage is below the high-warning-threshold
Configurable	False

high-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver voltage high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Description	Read from the installed transceiver
Configurable	False

latest-value *decimal-number*

Context	interface name <i>string</i> transceiver voltage latest-value <i>decimal-number</i>
Tree	latest-value
Description	The current voltage reading of the transceiver module (in Volts)
Configurable	False

low-alarm-condition *boolean*

Context	interface name <i>string</i> transceiver voltage low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Description	Set to true whenever the module voltage is below the low-alarm-threshold and set to false whenever the module voltage is above the low-alarm-threshold
Configurable	False

low-alarm-threshold *decimal-number*

Context	interface name <i>string</i> transceiver voltage low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Description	Read from the installed transceiver
Configurable	False

low-warning-condition *boolean*

Context	interface name <i>string</i> transceiver voltage low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Description	Set to true whenever the module voltage is below the low-warning-threshold and set to false whenever the module voltage is above the low-warning-threshold
Configurable	False

low-warning-threshold *decimal-number*

Context	interface name <i>string</i> transceiver voltage low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Description	Read from the installed transceiver
Configurable	False

wavelength *decimal-number*

Context	interface name <i>string</i> transceiver wavelength <i>decimal-number</i>
Tree	wavelength
Description	Wavelength of the transmitting laser in nanometers
Configurable	False

vlan-tagging *boolean*

Context	interface name <i>string</i> vlan-tagging <i>boolean</i>
Tree	vlan-tagging
Description	When set to true the interface is allowed to accept frames with one or more VLAN tags
Configurable	True

5 network-instance

- network-instance name** *string*
- + **admin-state** *keyword*
 - + **aft address-family** *string*
 - **entries**
 - **entry index** *number*
 - **match**
 - **state**
 - **ip-prefix** (*ipv4-prefix | ipv6-prefix*)
 - **preference** *number*
 - **next-hop index** *number*
 - **state**
 - **ip-address** *string*
 - **origin-protocol** (*identityref | string*)
 - + **aggregate-routes**
 - + **route prefix** (*ipv4-prefix | ipv6-prefix*)
 - + **admin-state** *keyword*
 - + **aggregator**
 - + **address** *string*
 - + **as-number** *number*
 - + **communities**
 - + **add** (*bgp-std-community-type | bgp-std-community-regexp-type | identityref | bgp-large-community-type | bgp-large-community-regexp-type*)
 - + **generate-icmp** *boolean*
 - **installed** *boolean*
 - + **summary-only** *boolean*
 - **bgp-rib**
 - **attr-sets**
 - **attr-set attr-set-type** *keyword index number*
 - **aggregator**
 - **address** (*ipv4-address | ipv6-address*)
 - **as-number** *number*
 - **aigp** *number*
 - **as-path**
 - **segment as-path-index** *number*
 - **member** *number*
 - **type** *keyword*
 - **atomic-aggregate** *boolean*
 - **cluster-list** (*ipv4-address | ipv6-address*)
 - **communities**
 - **community** *string*
 - **ext-community** *string*
 - **large-community** *string*
 - **local-pref** *number*
 - **med** *number*
 - **next-hop** (*ipv4-address | ipv6-address*)
 - **origin** *keyword*
 - **originator-id** (*ipv4-address | ipv6-address*)
 - **unknown-attributes**
 - **unknown-attribute unknown-attrib-index** *number*
 - **attr-len** *number*

- **attr-type** *number*
- **extended** *boolean*
- **optional** *boolean*
- **partial** *boolean*
- **transitive** *boolean*
- **ipv4-unicast**
 - **local-rib**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*
 - **attr-id** *reference*
 - **best-route** *boolean*
 - **invalid-reason**
 - **as-loop** *boolean*
 - **cluster-loop** *boolean*
 - **next-hop-unresolved** *boolean*
 - **rejected-route** *boolean*
 - **last-modified** *string*
 - **pending-delete** *boolean*
 - **stale-route** *boolean*
 - **tie-break-reason** *keyword*
 - **used-route** *boolean*
 - **valid-route** *boolean*
 - **rib-in-out**
 - **rib-in-post**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)
 - **attr-id** *reference*
 - **best-route** *boolean*
 - **invalid-reason**
 - **as-loop** *boolean*
 - **cluster-loop** *boolean*
 - **next-hop-unresolved** *boolean*
 - **rejected-route** *boolean*
 - **last-modified** *string*
 - **pending-delete** *boolean*
 - **stale-route** *boolean*
 - **tie-break-reason** *keyword*
 - **used-route** *boolean*
 - **valid-route** *boolean*
 - **rib-in-pre**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)
 - **attr-id** *reference*
 - **rib-out-post**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)
 - **attr-id** *reference*
- **ipv6-unicast**
 - **local-rib**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*
 - **attr-id** *reference*
 - **best-route** *boolean*
 - **invalid-reason**
 - **as-loop** *boolean*
 - **cluster-loop** *boolean*
 - **next-hop-unresolved** *boolean*
 - **rejected-route** *boolean*
 - **last-modified** *string*

- **pending-delete** *boolean*
- **stale-route** *boolean*
- **tie-break-reason** *keyword*
- **used-route** *boolean*
- **valid-route** *boolean*
- **rib-in-out**
 - **rib-in-post**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)
 - **attr-id** *reference*
 - **best-route** *boolean*
 - **invalid-reason**
 - **as-loop** *boolean*
 - **cluster-loop** *boolean*
 - **next-hop-unresolved** *boolean*
 - **rejected-route** *boolean*
 - **last-modified** *string*
 - **pending-delete** *boolean*
 - **stale-route** *boolean*
 - **tie-break-reason** *keyword*
 - **used-route** *boolean*
 - **valid-route** *boolean*
 - **rib-in-pre**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)
 - **attr-id** *reference*
 - **rib-out-post**
 - **routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)
 - **attr-id** *reference*
- + **bridge-table**
 - + **discard-unknown-dest-mac** *boolean*
 - + **mac-duplication**
 - + **action** *keyword*
 - + **admin-state** *keyword*
 - **duplicate-entries**
 - **mac address** *string*
 - **destination** *string*
 - **destination-index** *number*
 - **destination-type** *keyword*
 - **dup-detect-time** *string*
 - **hold-down-time-remaining** *number*
 - + **hold-down-time** *number*
 - + **monitoring-window** *number*
 - + **num-moves** *number*
 - + **mac-learning**
 - + **admin-state** *keyword*
 - + **aging**
 - + **admin-state** *keyword*
 - + **age-time** *number*
 - **learnt-entries**
 - **mac address** *string*
 - **aging** (*number | keyword*)
 - **destination** *string*
 - **last-update** *string*
 - **mac-relearn-only** *boolean*
 - **oper-mac-learning** *keyword*

- **oper-mac-learning-disabled-reason** *keyword*
- + **mac-limit**
 - + **maximum-entries** *number*
 - + **warning-threshold-pct** *number*
- **mac-table**
 - **mac address** *string*
 - **destination** *string*
 - **destination-index** *number*
 - **destination-type** *keyword*
 - **failed-slots** *number*
 - **last-update** *string*
 - **not-programmed-reason** *keyword*
 - **type** *keyword*
- + **static-mac**
 - + **mac address** *string*
 - + **destination** (*keyword | reference*)
- **statistics**
 - **active-entries** *number*
 - **mac-type type** *keyword*
 - **active-entries** *number*
 - **total-entries** *number*
 - **total-entries** *number*
- + **description** *string*
- + **icmp**
 - **statistics**
 - **last-clear** *string*
 - **total**
 - **in-error-packets** *number*
 - **in-packets** *number*
 - **out-error-packets** *number*
 - **out-packets** *number*
 - **type name** *keyword*
 - **in-packets** *number*
 - **out-packets** *number*
- + **icmp6**
 - **statistics**
 - **last-clear** *string*
 - **total**
 - **in-error-packets** *number*
 - **in-packets** *number*
 - **out-error-packets** *number*
 - **out-packets** *number*
 - **type name** *keyword*
 - **in-packets** *number*
 - **out-packets** *number*
- + **interface name** *string*
 - **index** *number*
 - **mac-relearn-only** *boolean*
 - **oper-down-reason** *keyword*
 - **oper-mac-learning** *keyword*
 - **oper-mac-learning-disabled-reason** *keyword*
 - **oper-state** *keyword*
- + **ip-forwarding**
 - + **receive-ipv4-check** *boolean*

- + **receive-ipv6-check** *boolean*
- + **ip-load-balancing**
 - + **resilient-hash-prefix ip-prefix** (*ipv4-prefix | ipv6-prefix*)
 - + **hash-buckets-per-path** *number*
 - + **max-paths** *number*
- + **mpls**
 - + **admin-state** *keyword*
 - + **static-mpls-entry top-label** (*number | keyword*)
 - + **collect-stats** *boolean*
 - **installed** *boolean*
 - + **next-hop-group** *reference*
 - + **operation** *keyword*
 - **origin-protocol** *identityref*
 - + **preference** *number*
 - + **ttl-propagation** *boolean*
- + **mtu**
 - + **path-mtu-discovery** *boolean*
- + **next-hop-groups**
 - + **group name** *string*
 - + **admin-state** *keyword*
 - + **blackhole**
 - + **generate-icmp** *boolean*
 - + **nexthop index** *number*
 - + **admin-state** *keyword*
 - + **ip-address** (*ipv4-address | ipv6-address*)
 - + **pushed-mpls-label-stack** (*number | keyword*)
 - + **resolve** *boolean*
- **oper-mac-vrf-mtu** *number*
- **oper-state** *keyword*
- + **protocols**
 - + **bgp**
 - + **admin-state** *keyword*
 - + **as-path-options**
 - + **allow-own-as** *number*
 - + **remove-private-as**
 - + **ignore-peer-as** *boolean*
 - + **leading-only** *boolean*
 - + **mode** *keyword*
 - + **authentication**
 - + **keychain** *reference*
 - + **autonomous-system** *number*
 - + **convergence**
 - + **min-wait-to-advertise** *number*
 - + **dynamic-neighbors**
 - + **accept**
 - + **match prefix** (*ipv4-prefix | ipv6-prefix*) **group-id-range** *string*
 - + **allowed-peer-as** *string*
 - + **peer-group** *reference*
 - + **max-sessions** *number*
 - + **initiate**
 - + **match prefix** (*ipv4-prefix | ipv6-prefix*) **group-id-range** *string*
 - + **allowed-peer-as** *string*
 - + **peer-group** *reference*
 - + **max-sessions** *number*

- + **ebgp-default-policy**
 - + **export-reject-all** *boolean*
 - + **import-reject-all** *boolean*
- + **export-policy** *reference*
- + **failure-detection**
 - + **enable-bfd** *boolean*
 - + **fast-failover** *boolean*
- + **graceful-restart**
 - + **admin-state** *keyword*
 - + **stale-routes-time** *number*
- + **group group-name** *string*
 - + **admin-state** *keyword*
 - + **as-path-options**
 - + **allow-own-as** *number*
 - + **remove-private-as**
 - + **ignore-peer-as** *boolean*
 - + **leading-only** *boolean*
 - + **mode** *keyword*
 - + **replace-peer-as** *boolean*
 - + **authentication**
 - + **keychain** *reference*
 - + **description** *string*
 - + **export-policy** *reference*
 - + **failure-detection**
 - + **enable-bfd** *boolean*
 - + **fast-failover** *boolean*
 - + **graceful-restart**
 - + **admin-state** *keyword*
 - + **stale-routes-time** *number*
 - + **import-policy** *reference*
 - + **ipv4-unicast**
 - + **admin-state** *keyword*
 - + **advertise-ipv6-next-hops** *boolean*
 - + **prefix-limit**
 - + **max-received-routes** *number*
 - + **warning-threshold-pct** *number*
 - + **receive-ipv6-next-hops** *boolean*
 - + **ipv6-unicast**
 - + **admin-state** *keyword*
 - + **prefix-limit**
 - + **max-received-routes** *number*
 - + **warning-threshold-pct** *number*
 - + **local-as as-number** *number*
 - + **prepend-global-as** *boolean*
 - + **prepend-local-as** *boolean*
 - + **local-preference** *number*
 - **maintenance-group** *string*
 - + **next-hop-self** *boolean*
 - + **peer-as** *number*
 - + **route-reflector**
 - + **client** *boolean*
 - + **cluster-id** *string*
 - + **send-community**
 - + **large** *boolean*

- + **standard** *boolean*
- + **send-default-route**
 - + **export-policy** *reference*
 - + **ipv4-unicast** *boolean*
 - + **ipv6-unicast** *boolean*
- **statistics**
 - **disabled-peers** *number*
 - **dynamic-peers** *number*
 - **path-memory** *number*
 - **total-active-routes** *number*
 - **total-paths** *number*
 - **total-peers** *number*
 - **total-prefixes** *number*
 - **total-received-routes** *number*
 - **up-peers** *number*
- + **timers**
 - + **connect-retry** *number*
 - + **hold-time** *number*
 - + **keepalive-interval** *number*
 - + **minimum-advertisement-interval** *number*
- + **trace-options**
 - + **flag name** *keyword*
 - + **modifier** *keyword*
- + **transport**
 - + **local-address** (*ipv4-address | ipv6-address*)
 - + **passive-mode** *boolean*
 - + **tcp-mss** *number*
 - **under-maintenance** *boolean*
- + **import-policy** *reference*
- + **ipv4-unicast**
 - **active-routes** *number*
 - + **admin-state** *keyword*
 - + **advertise-ipv6-next-hops** *boolean*
 - + **convergence**
 - **converged-peers** *number*
 - **convergence-state** *keyword*
 - **convergence-time** *number*
 - **first-up-peer-time** *number*
 - **last-up-peer-time** *number*
 - + **max-wait-to-advertise** *number*
 - **oper-max-wait-to-advertise** *number*
 - **up-peers** *number*
 - **up-peers-when-min-expired** *number*
- + **multipath**
 - + **allow-multiple-as** *boolean*
 - + **max-paths-level-1** *number*
 - + **max-paths-level-2** *number*
 - + **receive-ipv6-next-hops** *boolean*
 - **received-routes** *number*
- + **ipv6-unicast**
 - **active-routes** *number*
 - + **admin-state** *keyword*
 - + **convergence**
 - **converged-peers** *number*

- **convergence-state** *keyword*
- **convergence-time** *number*
- **first-up-peer-time** *number*
- **last-up-peer-time** *number*
- + **max-wait-to-advertise** *number*
- **oper-max-wait-to-advertise** *number*
- **up-peers** *number*
- **up-peers-when-min-expired** *number*
- + **multipath**
 - + **allow-multiple-as** *boolean*
 - + **max-paths-level-1** *number*
 - + **max-paths-level-2** *number*
- **received-routes** *number*
- + **local-preference** *number*
- **maintenance-group** *string*
- + **neighbor peer-address** (*ipv4-address* | *ipv6-address*)
- + **admin-state** *keyword*
- **advertised-capabilities** *keyword*
- + **as-path-options**
 - + **allow-own-as** *number*
 - + **remove-private-as**
 - + **ignore-peer-as** *boolean*
 - + **leading-only** *boolean*
 - + **mode** *keyword*
 - + **replace-peer-as** *boolean*
- + **authentication**
 - + **keychain** *reference*
- + **description** *string*
- **discovered-by-lldp** *boolean*
- **dynamic-neighbor** *boolean*
- **established-transitions** *number*
- + **export-policy** *reference*
- + **failure-detection**
 - + **enable-bfd** *boolean*
 - + **fast-failover** *boolean*
- + **graceful-restart**
 - + **admin-state** *keyword*
 - **helper-active** *boolean*
 - **last-restart-time** *string*
 - **neighbor-capability**
 - **afi-safi name** *keyword*
 - **forwarding-preserved** *boolean*
 - **restart-time** *number*
 - **number-of-restarts** *number*
 - + **stale-routes-time** *number*
- + **import-policy** *reference*
- + **ipv4-unicast**
 - **active-routes** *number*
 - + **admin-state** *keyword*
 - + **advertise-ipv6-next-hops** *boolean*
 - **oper-state** *keyword*
 - + **prefix-limit**
 - + **max-received-routes** *number*
 - + **warning-threshold-pct** *number*

- + **receive-ipv6-next-hops** *boolean*
- **received-routes** *number*
- **rejected-routes** *number*
- **sent-routes** *number*
- + **ipv6-unicast**
 - **active-routes** *number*
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - + **prefix-limit**
 - + **max-received-routes** *number*
 - + **warning-threshold-pct** *number*
 - **received-routes** *number*
 - **rejected-routes** *number*
 - **sent-routes** *number*
- **last-established** *string*
- **last-event** *keyword*
- **last-notification-error-code** *keyword*
- **last-notification-error-subcode** *keyword*
- **last-state** *keyword*
- + **local-as as-number** *number*
 - + **prepend-global-as** *boolean*
 - + **prepend-local-as** *boolean*
- + **local-preference** *number*
- **maintenance-group** *string*
- + **next-hop-self** *boolean*
- + **peer-as** *number*
- + **peer-group** *reference*
- **received-afi-safi** *keyword*
- **received-capabilities** *keyword*
- **received-end-of-rib** *keyword*
- **received-messages**
 - **keepalives** *number*
 - **last-notification-time** *string*
 - **last-update-time** *string*
 - **malformed-updates** *number*
 - **notifications** *number*
 - **opens** *number*
 - **queue-depth** *number*
 - **route-refresh** *number*
 - **total-messages** *number*
 - **total-non-updates** *number*
 - **total-updates** *number*
- + **route-reflector**
 - + **client** *boolean*
 - + **cluster-id** *string*
- + **send-community**
 - + **large** *boolean*
 - + **standard** *boolean*
- + **send-default-route**
 - + **export-policy** *reference*
 - + **ipv4-unicast** *boolean*
 - + **ipv6-unicast** *boolean*
- **sent-end-of-rib** *keyword*
- **sent-messages**

- **keepalives** *number*
- **last-notification-time** *string*
- **notifications** *number*
- **opens** *number*
- **queue-depth** *number*
- **route-refresh** *number*
- **total-messages** *number*
- **total-non-updates** *number*
- **total-updates** *number*
- **session-state** *keyword*
- **slow-peer** *keyword*
- + **timers**
 - + **connect-retry** *number*
 - + **hold-time** *number*
 - + **keepalive-interval** *number*
 - + **minimum-advertisement-interval** *number*
 - **negotiated-hold-time** *number*
 - **negotiated-keepalive-interval** *number*
 - **next-connect-retry-time** *string*
- + **trace-options**
 - + **flag name** *keyword*
 - + **modifier** *keyword*
- + **transport**
 - + **local-address** (*ipv4-address* | *ipv6-address*)
 - **local-port** *number*
 - + **passive-mode** *boolean*
 - **remote-port** *number*
 - + **tcp-mss** *number*
 - **under-maintenance** *boolean*
- **oper-state** *keyword*
- + **preference**
 - + **ebgp** *number*
 - + **ibgp** *number*
- + **route-advertisement**
 - + **rapid-withdrawal** *boolean*
 - + **wait-for-fib-install** *boolean*
- + **route-reflector**
 - + **client** *boolean*
 - + **cluster-id** *string*
- + **router-id** *string*
- + **send-community**
 - + **large** *boolean*
 - + **standard** *boolean*
- **statistics**
 - **disabled-peers** *number*
 - **dynamic-peers** *number*
 - **path-memory** *number*
 - **total-active-routes** *number*
 - **total-paths** *number*
 - **total-peers** *number*
 - **total-prefixes** *number*
 - **total-received-routes** *number*
 - **up-peers** *number*
- + **trace-options**

- + **flag name** *keyword*
- + **modifier** *keyword*
- + **transport**
- + **tcp-mss** *number*
- **under-maintenance** *boolean*
- + **isis**
- + **instance name** *string*
- + **admin-state** *keyword*
- + **attached-bit**
- + **ignore** *boolean*
- + **suppress** *boolean*
- + **authentication**
- + **csnp-authentication** *boolean*
- + **hello-authentication** *boolean*
- + **keychain** *reference*
- + **psnp-authentication** *boolean*
- + **auto-cost**
- + **reference-bandwidth** *number*
- + **export-policy** *reference*
- + **graceful-restart**
- + **helper-mode** *boolean*
- + **inter-level-propagation-policies**
- + **level1-to-level2**
- + **summary-address ip-prefix** (*ipv4-prefix | ipv6-prefix*)
- + **route-tag** *number*
- + **interface interface-name** *reference*
- **adjacency neighbor-system-id** *string adjacency-level string*
- **down-reason** *keyword*
- **last-up-down-transition** *string*
- **neighbor-circuit-type** *keyword*
- **neighbor-hostname** *string*
- **neighbor-ipv4** *string*
- **neighbor-ipv6** *string*
- **neighbor-last-restart** (*keyword | date-and-time-delta*)
- **neighbor-priority** *number*
- **neighbor-restart-capable** *boolean*
- **neighbor-restart-status** *keyword*
- **neighbor-restarts** *number*
- **neighbor-snpa** *string*
- **remaining-holdtime** *number*
- **state** *keyword*
- **up-down-transitions** *number*
- + **admin-state** *keyword*
- + **authentication**
- + **hello-authentication** *boolean*
- + **keychain** *reference*
- **circuit-id** *number*
- + **circuit-type** *keyword*
- + **hello-padding** *keyword*
- + **ipv4-unicast**
- + **admin-state** *keyword*
- + **enable-bfd** *boolean*
- + **include-bfd-tlv** *boolean*
- + **ipv6-unicast**

- + **admin-state** *keyword*
- + **enable-bfd** *boolean*
- + **include-bfd-tlv** *boolean*
- + **level level-number** *number*
 - + **authentication**
 - + **keychain** *reference*
 - + **disable** *boolean*
 - + **ipv6-unicast-metric** *number*
 - + **metric** *number*
 - + **priority** *number*
 - + **timers**
 - + **hello-interval** *number*
 - + **hello-multiplier** *number*
- **oper-state** *keyword*
- + **passive** *boolean*
- + **timers**
 - + **csnp-interval** *number*
 - + **lsp-pacing-interval** *number*
- + **trace-options**
 - + **trace** *keyword*
- + **ipv4-unicast**
 - + **admin-state** *keyword*
- + **ipv6-unicast**
 - + **admin-state** *keyword*
 - + **multi-topology** *boolean*
- + **level level-number** *number*
 - + **authentication**
 - + **csnp-authentication** *boolean*
 - + **hello-authentication** *boolean*
 - + **keychain** *reference*
 - + **psnp-authentication** *boolean*
 - + **metric-style** *keyword*
 - + **route-preference**
 - + **external** *number*
 - + **internal** *number*
 - + **trace-options**
 - + **trace** *keyword*
- + **level-capability** *keyword*
- **level-database level-number** *number* **lsp-id** *string*
 - **attributes**
 - **attached** *boolean*
 - **level1-is-type** *boolean*
 - **level2-is-type** *boolean*
 - **overload** *boolean*
 - **checksum** *string*
 - **defined-tlvs**
 - **area-addresses** *string*
 - **authentication**
 - **auth-data** *string*
 - **auth-type** *keyword*
 - **extended-ipv4-reachability ipv4-prefix** *string*
 - **down** *boolean*
 - **metric** *number*
 - **extended-is-reachability neighbor** *string*

- **default-metric** *number*
- **sub-tlvs**
 - **ipv4-interface-address** *string*
- **hostname** *string*
- **ipv4-external-reachability ipv4-prefix** *string*
 - **default-metric** *number*
 - **default-metric-type** *keyword*
 - **down** *boolean*
- **ipv4-interface-addresses** (*ipv4-address | ipv6-address*)
- **ipv4-internal-reachability ipv4-prefix** *string*
 - **default-metric** *number*
 - **default-metric-type** *keyword*
 - **down** *boolean*
- **ipv6-interface-addresses** (*ipv4-address | ipv6-address*)
- **ipv6-reachability ipv6-prefix** *string*
 - **down** *boolean*
 - **external** *boolean*
 - **metric** *number*
- **is-reachability neighbor** *string*
 - **default-metric** *number*
 - **default-metric-type** *keyword*
- **mt-ipv4-reachability ipv4-prefix** *string*
 - **down** *boolean*
 - **metric** *number*
 - **mt-id** *number*
- **mt-ipv6-reachability ipv6-prefix** *string*
 - **down** *boolean*
 - **external** *boolean*
 - **metric** *number*
 - **mt-id** *number*
- **mt-is-reachability neighbor** *string*
 - **default-metric** *number*
 - **mt-id** *number*
- **multi-topology**
 - **topology mt-id** *number*
 - **attached** *boolean*
 - **overload** *boolean*
- **nlpid** *keyword*
- **purge-oi** *string*
- **maximum-area-addresses** *number*
- **pdu-length** *number*
- **pdu-type** *number*
- **pkt-version** *number*
- **remaining-lifetime** *number*
- **sequence-number** *string*
- **system-id-len** *number*
- **undefined-tlvs** *string*
- **version** *number*
- + **max-ecmp-paths** *number*
- + **net** *string*
- **oper-state** *keyword*
- **oper-system-id** *string*
- + **overload**
 - + **advertise-external** *boolean*

- + **advertise-interlevel** *boolean*
- + **immediate**
 - + **max-metric** *boolean*
 - + **set-bit** *boolean*
- + **on-boot**
 - + **max-metric** *boolean*
 - + **set-bit** *boolean*
 - + **timeout** *number*
- + **poi-tlv** *boolean*
- **statistics**
 - **last-partial-spf** *string*
 - **last-spf** *string*
 - **partial-spf-runs** *number*
 - **pdu pdu-name** *keyword*
 - **dropped** *number*
 - **processed** *number*
 - **received** *number*
 - **retransmitted** *number*
 - **sent** *number*
 - **spf-runs** *number*
- + **timers**
 - + **lsp-generation**
 - + **initial-wait** *number*
 - + **max-wait** *number*
 - + **second-wait** *number*
 - + **lsp-lifetime** *number*
 - + **lsp-refresh**
 - + **half-lifetime** *boolean*
 - + **interval** *number*
 - + **spf**
 - + **initial-wait** *number*
 - + **max-wait** *number*
 - + **second-wait** *number*
- + **trace-options**
 - + **trace** *keyword*
- + **transport**
 - + **lsp-mtu-size** *number*
- + **linux**
 - + **export-neighbors** *boolean*
 - + **export-routes** *boolean*
 - + **import-routes** *boolean*
- + **ospfv2**
 - + **instance name** *string*
 - + **admin-state** *keyword*
 - + **advertise-router-capability** *keyword*
 - + **area area-id** *string*
 - + **advertise-router-capability** *boolean*
 - + **area-range ip-prefix-mask** *string*
 - + **advertise** *boolean*
 - + **blackhole-aggregate** *boolean*
 - + **export-policy** *reference*
 - + **interface interface-name** *reference*
 - + **admin-state** *keyword*
 - + **advertise-router-capability** *boolean*

- + **advertise-subnet** *boolean*
- + **authentication**
 - + **keychain** *reference*
- **bad-packets**
 - **bad-area** *number*
 - **bad-auth-type** *number*
 - **bad-checksum** *number*
 - **bad-dead-interval** *number*
 - **bad-dest-address** *number*
 - **bad-hello-interval** *number*
 - **bad-length** *number*
 - **bad-neighbors** *number*
 - **bad-network** *number*
 - **bad-options** *number*
 - **bad-packet-type** *number*
 - **bad-version** *number*
 - **bad-virtual-link** *number*
- **bdr-id** *string*
- + **dead-interval** *number*
- **dr-id** *string*
- **events** *number*
- + **failure-detection**
 - + **enable-bfd** *boolean*
- + **hello-interval** *number*
- + **interface-type** *keyword*
- **last-enabled-time** *string*
- **last-event-time** *string*
- **link-lsa-cksum-sum** *number*
- **link-lsa-count** *number*
- **local-ip-address** *string*
- + **lsa-filter-out** *keyword*
- + **metric** *number*
- + **mtu** *number*
- **neighbor router-id** *string*
 - **adjacency-state** *identityref*
 - **backup-designated-router** *string*
 - **dead-time** *number*
 - **designated-router** *string*
 - **last-established-time** *number*
 - **optional-capabilities** *string*
 - **priority** *number*
 - **retransmission-queue-length** *number*
 - **state-changes** *number*
- **neighbor-count** *number*
- **oper-metric** *number*
- **oper-mtu** *number*
- **oper-state** *keyword*
- **packets**
 - **discarded** *number*
 - **retransmits** *number*
 - **rx-db-description** *number*
 - **rx-hello** *number*
 - **rx-ls-ack** *number*
 - **rx-ls-request** *number*

- **rx-ls-update** *number*
- **rx-total** *number*
- **tx-db-description** *number*
- **tx-hello** *number*
- **tx-ls-ack** *number*
- **tx-ls-request** *number*
- **tx-ls-update** *number*
- **tx-total** *number*
- + **passive** *boolean*
- + **priority** *number*
- + **retransmit-interval** *number*
- + **transit-delay** *number*
- **type** *keyword*
- + **nssa**
 - + **area-range ip-prefix-mask** *string*
 - + **advertise** *boolean*
 - + **originate-default-route**
 - + **adjacency-check** *boolean*
 - + **type-nssa** *boolean*
 - + **redistribute-external** *boolean*
 - + **summaries** *boolean*
- + **stub**
 - + **default-metric** *number*
 - + **summaries** *boolean*
- **area-border-router** *boolean*
- **as-border-router** *boolean*
- + **asbr**
 - + **trace-path** (*number* | *keyword*)
- **backbone-router** *boolean*
- + **export-limit**
 - + **log-percent** *number*
 - + **number** *number*
- + **export-policy** *reference*
- + **external-db-overflow**
 - + **interval** *number*
 - + **limit** *number*
- + **external-preference** *number*
- + **graceful-restart**
 - + **helper-mode** *boolean*
 - + **strict-lsa-checking** *boolean*
- **last-disabled-reason** *string*
- **last-enabled-time** *string*
- **last-overflow-entered-time** *string*
- **last-overflow-exit-time** *string*
- **last-overload-enter-code** *keyword*
- **last-overload-entered-time** *string*
- **last-overload-exit-code** *keyword*
- **last-overload-exit-time** *string*
- + **log-adjacency-changes** *boolean*
- + **max-ecmp-paths** *number*
- **oper-router-id** *string*
- **oper-state** *keyword*
- **overflow** *boolean*
- + **overload**

- + **active** *boolean*
- + **overload-include-ext-1** *boolean*
- + **overload-include-ext-2** *boolean*
- + **overload-include-ext-stub** *boolean*
- + **overload-on-boot**
 - + **timeout** *number*
- + **rtr-adv-lsa-limit**
 - + **log-only** *boolean*
 - + **max-lsa-count** *number*
 - + **overload-timeout** *number*
 - + **warning-threshold** *number*
- **overload-rem-interval** *number*
- **overload-state** *keyword*
- **ovld-lsa-limit-rem-interval** *number*
- + **preference** *number*
- + **reference-bandwidth** *number*
- + **router-id** *string*
- **routes-submitted** *number*
- **spf**
 - **avg-spf-run-interval** *number*
 - **ext-spf-runs** *number*
 - **full-spf-runs** *number*
 - **incremental-ext-spf-runs** *number*
 - **incremental-inter-spf-runs** *number*
 - **last-ext-spf**
 - **interval** *number*
 - **run-time** *string*
 - **last-full-spf**
 - **extern-spf-time** *number*
 - **inter-spf-time** *number*
 - **intra-spf-time** *number*
 - **rtm-update-time** *number*
 - **run-time** *string*
 - **total-time** *number*
 - **max-spf-run-interval** *number*
 - **min-spf-run-interval** *number*
 - **spf-attempts-failed** *number*
- + **timers**
 - + **incremental-spf-wait** *number*
 - + **lsa-accumulate** *number*
 - + **lsa-arrival** *number*
 - + **lsa-generate**
 - + **lsa-initial-wait** *number*
 - + **lsa-second-wait** *number*
 - + **max-lsa-wait** *number*
 - + **redistribute-delay** *number*
 - + **spf-wait**
 - + **spf-initial-wait** *number*
 - + **spf-max-wait** *number*
 - + **spf-second-wait** *number*
 - **total-exported-routes** *number*
- **route-table**
 - **ipv4-unicast**
 - **route ipv4-prefix** *string id number*

- **active** *boolean*
- **fib-programming**
 - **failed-slots** *number*
 - **status** *keyword*
- **last-app-update** *string*
- **metric** *number*
- **next-hop-group** *reference*
- **owner** *identityref*
- **preference** *number*
- **resilient-hash** *boolean*
- **statistics**
 - **active-entries** *number*
 - **active-entries-with-ecmp** *number*
 - **total-entries** *number*
- **ipv6-unicast**
 - **route ipv6-prefix** *string id number*
 - **active** *boolean*
 - **fib-programming**
 - **failed-slots** *number*
 - **status** *keyword*
 - **last-app-update** *string*
 - **metric** *number*
 - **next-hop-group** *reference*
 - **owner** *identityref*
 - **preference** *number*
 - **resilient-hash** *boolean*
 - **statistics**
 - **active-entries** *number*
 - **active-entries-with-ecmp** *number*
 - **total-entries** *number*
- **mpls**
 - **route label** (*number | keyword*) **id** *number*
 - **active** *boolean*
 - **fib-change-pending** *boolean*
 - **last-app-update** *string*
 - **next-hop-group** *reference*
 - **owner** *identityref*
 - **preference** *number*
 - **statistics**
 - **active-entries** *number*
 - **active-entries-with-ecmp** *number*
 - **total-entries** *number*
- **next-hop index** *number*
 - **encapsulate-header** *keyword*
 - **ip-address** (*ipv4-address | ipv6-address*)
 - **pushed-mpls-label-stack** (*number | keyword*)
 - **resolving-route**
 - **ip-prefix** (*ipv4-prefix | ipv6-prefix*)
 - **owner** *identityref*
 - **subinterface** *reference*
 - **type** *identityref*
- **next-hop-group index** *number*
 - **last-app-update** *string*
 - **next-hop id** *number*

- **active** *boolean*
- **next-hop** *reference*
- **owner** *identityref*
- + **router-id** *string*
- + **static-routes**
 - + **route prefix** (*ipv4-prefix | ipv6-prefix*)
 - + **admin-state** *keyword*
 - **installed** *boolean*
 - + **metric** *number*
 - + **next-hop-group** *reference*
 - + **preference** *number*
- **tcp**
 - **connection local-address** (*ipv4-address | ipv6-address*) **local-port** *number* **remote-address** (*ipv4-address | ipv6-address*) **remote-port** *number*
 - **process-id** *number*
 - **session-state** *keyword*
 - **listening-application local-address** (*ipv4-address | ipv6-address*) **local-port** *number*
 - **process-id** *number*
 - **statistics**
 - **active-opens** *number*
 - **attempt-fails** *number*
 - **established-resets** *number*
 - **in-checksum-errors** *number*
 - **in-error-segments** *number*
 - **in-segments** *number*
 - **out-rst-segments** *number*
 - **out-segments** *number*
 - **passive-opens** *number*
 - **retransmitted-segments** *number*
- + **type** *identityref*
- **udp**
 - **listening-application local-address** (*ipv4-address | ipv6-address*) **local-port** *number*
 - **process-id** *number*
 - **statistics**
 - **ignored-multicast-packets** *number*
 - **in-checksum-errors** *number*
 - **in-error-packets** *number*
 - **in-no-open-ports-packets** *number*
 - **in-packets** *number*
 - **out-packets** *number*
 - **receive-buffer-errors** *number*
 - **send-buffer-errors** *number*

5.1 network-instance Descriptions

network-instance **name** *string*

Context	network-instance name <i>string</i>
Tree	network-instance
Description	Network instances configured on the local system
Configurable	True

name *string*

Context	network-instance name <i>string</i>
Description	A unique name identifying the network instance
String Length	1 to 255
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	This leaf contains the configured, desired state of the network instance.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

aft address-family *string*

Context	network-instance name <i>string</i> aft address-family <i>string</i>
Tree	aft
Description	An individual abstract forwarding table associated with a an address family within the network instance. The abstract forwarding tables (AFTs) that are associated with the network instance. An AFT is instantiated per-protocol running within the network-instance - such that one exists for IPv4 Unicast, IPv6 Unicast, MPLS, L2 forwarding entries, etc. A forwarding entry within the FIB has a set of next-hops, which may be a reference to an entry within another table - e.g., where a Layer 3 next-hop has an associated Layer 2 forwarding entry.
Configurable	True

address-family *string*

Context	network-instance name <i>string</i> aft address-family <i>string</i>
Description	Reference to the address family with which the AFT is associated
Configurable	True

entries

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries
Tree	entries
Description	Enclosing container for a list of abstract forwarding table entries within the network instance for a particular protocol (e.g., IPv4, IPv6, MPLS).
Configurable	False

entry [index](#) *number*

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i>
Tree	entry
Description	A forwarding database entry within the network instance
Configurable	False

[index](#) *number*

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i>
Description	A pointer to the index of the AFT entry within the network instance
Configurable	False

match

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> match
Tree	match
Description	Match criteria for the AFT entry
Configurable	False

state

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> match state
Tree	state
Description	Operational state parameters for match criteria of the AFT entry
Configurable	False

ip-prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> match state ip-prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	ip-prefix
Description	The IP prefix that the forwarding entry matches. Used for Layer 3 forwarding entries.
Configurable	False

preference *number*

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> match state preference <i>number</i>
Tree	preference
Description	Preference of the Route.
Configurable	False

next-hop **index** *number*

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> next-hop index <i>number</i>
Tree	next-hop
Description	A next-hop associated with the forwarding instance. The entries within the next-hop list should only reflect next-hops that are actively used by the local system. That is to say inactive, backup or FRR next-hops should not be included within this list.
Configurable	False

index *number*

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> next-hop index <i>number</i>
Description	A unique index identifying the next-hop entry for the AFT entry
Configurable	False

state

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> next-hop index <i>number</i> state
Tree	state
Description	Operational state parameters relating to the AFT next-hop entry
Configurable	False

ip-address *string*

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> next-hop index <i>number</i> state ip-address <i>string</i>
Tree	ip-address
Description	The IP address of the next-hop system.
Configurable	False

origin-protocol (*identityref | string*)

Context	network-instance name <i>string</i> aft address-family <i>string</i> entries entry index <i>number</i> next-hop index <i>number</i> state origin-protocol (<i>identityref string</i>)
Tree	origin-protocol
Description	The protocol from which the AFT entry was learned.
Options	<ul style="list-style-type: none">• <code>bgp</code> BGP• <code>isis</code> IS-IS• <code>ospf</code> OSPFv2• <code>ospf3</code> OSPFv3• <code>static</code> Locally-installed static route• <code>directly_connected</code> A directly connected route• <code>local</code> A local route• <code>local_aggregate</code> Locally defined aggregate route
Configurable	False

aggregate-routes

Context	network-instance name <i>string</i> aggregate-routes
Tree	aggregate-routes
Description	
Configurable	True

route prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	route
Description	
Configurable	True
Max. Elements	16384

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>)
Description	
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) admin-state <i>keyword</i>
Tree	admin-state
Description	This leaf contains the configured, desired state of the aggregate prefix.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

aggregator

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) aggregator
Tree	aggregator
Description	
Configurable	True

address *string*

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) aggregator address <i>string</i>
Tree	address
Description	Specifies the aggregator's IP address.
Configurable	True

as-number *number*

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) aggregator as-number <i>number</i>
Tree	as-number
Description	Specifies the aggregator's ASN
Range	1 to 4294967295
Configurable	True

communities

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) communities
Tree	communities
Description	
Configurable	True

add (*bgp-std-community-type | bgp-std-community-regexp-type | identityref | bgp-large-community-type | bgp-large-community-regexp-type*)

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) communities add (<i>bgp-std-community-type bgp-std-community-regexp-type identityref bgp-large-community-type bgp-large-community-regexp-type</i>)
Tree	add
Description	
Options	<ul style="list-style-type: none">• no-export Do not export NLRI received carrying this community outside the bounds of this autonomous system, or this confederation if the local autonomous system is a confederation member AS. This community has a value of 0xFFFFFFFF01.• no-advertise All NLRI received carrying this community must not be advertised to other BGP peers. This community has a value of 0xFFFFFFFF02.• no-export-subconfed All NLRI received carrying this community must not be advertised to external BGP peers - including over confederation sub-AS boundaries. This community has a value of 0xFFFFFFFF03.
Configurable	True
Max. Elements	12

generate-icmp *boolean*

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) generate-icmp <i>boolean</i>
Tree	generate-icmp
Description	When set to true the router generates ICMP unreachable messages for packets matching the aggregate route (and not a more specific route).
Configurable	True

installed *boolean*

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) installed <i>boolean</i>
Tree	installed
Description	If set to true, this indicates that the aggregate route was installed into the datapath. If this is false then there are 2 possible reasons: (a) the admin-state is disable (b) there is another IP route for the same prefix that has a superior preference
Configurable	False

summary-only *boolean*

Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) summary-only <i>boolean</i>
Tree	summary-only
Description	When set to true the router blocks the advertisement of all contributing routes of this aggregate route in dynamic protocols such as BGP.
Default	false
Configurable	True

bgp-rib

Context	network-instance name <i>string</i> bgp-rib
Tree	bgp-rib
Description	Container for BGP RIB state.
Configurable	False

attr-sets

Context	network-instance name <i>string</i> bgp-rib attr-sets
Tree	attr-sets
Description	Container for BGP RIB path attribute sets that can be shared by one or more BGP routes.
Configurable	False

attr-set **attr-set-type** *keyword* **index** *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Tree	attr-set
Description	List of attribute sets.
Configurable	False

attr-set-type *keyword*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Description	The type of the attribute-set. RIB-IN attribute sets can only be referenced by BGP routes in the RIB-IN. RIB-OUT attribute sets can only be referenced by BGP routes in the RIB-OUT.
Options	<ul style="list-style-type: none">rib-in

Configurable • rib-out
False

index number

Context **network-instance name** *string* **bgp-rib attr-sets attr-set attr-set-type** *keyword* **index number**

Description A unique internal identifier of the attribute set.

Configurable False

aggregator

Context **network-instance name** *string* **bgp-rib attr-sets attr-set attr-set-type** *keyword* **index number aggregator**

Tree **aggregator**

Description

Configurable False

address (*ipv4-address | ipv6-address*)

Context **network-instance name** *string* **bgp-rib attr-sets attr-set attr-set-type** *keyword* **index number aggregator address** (*ipv4-address | ipv6-address*)

Tree **address**

Description The router ID of the BGP router that formed the aggregate route.

Configurable False

as-number number

Context **network-instance name** *string* **bgp-rib attr-sets attr-set attr-set-type** *keyword* **index number aggregator as-number** *number*

Tree **as-number**

Description The 2byte or 4byte AS number of the router that formed the aggregate route.

Range 1 to 4294967295

Configurable False

aigp *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number aigp number</i>
Tree	aigp
Description	The value in the AIGP path attribute.
Configurable	False

as-path

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number as-path</i>
Tree	as-path
Description	A container for the AS path attribute of the attribute set.
Configurable	False

segment as-path-index *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number as-path segment as-path-index number</i>
Tree	segment
Description	A list of segments. Each segment has a type and a list of one or more AS numbers.
Configurable	False

as-path-index *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number as-path segment as-path-index number</i>
Description	RIB attribute AS Path index
Configurable	False

member *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number as-path segment as-path-index number member number</i>
Tree	member
Description	A list of AS numbers (each of which is a 2byte-ASN or a 4byte-ASN) that belong to the AS path segment.
Range	1 to 4294967295
Configurable	False

type *keyword*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> as-path segment as-path-index <i>number</i> type <i>keyword</i>
Tree	type
Description	The type of the AS path segment.
Options	<ul style="list-style-type: none">• as-set• as-sequence• as-confed-sequence• as-confed-set
Configurable	False

atomic-aggregate *boolean*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> atomic-aggregate <i>boolean</i>
Tree	atomic-aggregate
Description	Set to true to indicate the presence of the ATOMIC_AGGREGATE path attribute.
Configurable	False

cluster-list (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> cluster-list (<i>ipv4-address ipv6-address</i>)
Tree	cluster-list
Description	The list of IPv4 addresses in the CLUSTER_LIST path attribute.
Configurable	False

communities

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> communities
Tree	communities
Description	
Configurable	False

community *string*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number communities community string</i>
Tree	community
Description	List of standard 4-byte community values in the COMMUNITY path attribute. Each should be displayed in the format <0..65355>:<0..65535>
Configurable	False

ext-community *string*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number communities ext-community string</i>
Tree	ext-community
Description	List of extended 8-byte community values in the COMMUNITY path attribute.
Configurable	False

large-community *string*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number communities large-community string</i>
Tree	large-community
Description	List of large 12-byte community values in the LARGE_COMMUNITY path attribute. Each should be displayed in the format: <0..4294967295>:<0..4294967295>:< 0..4294967295>
String Length	1 to 72
Configurable	False

local-pref *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number local-pref number</i>
Tree	local-pref
Description	The value of the LOCAL_PREF path attribute.
Configurable	False

med *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> med <i>number</i>
Tree	med
Description	The value of the MULTI_EXIT_DISC path attribute.
Configurable	False

next-hop (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> next-hop (<i>ipv4-address ipv6-address</i>)
Tree	next-hop
Description	The IPv4 or IPv6 address of the BGP next-hop (extracted from the NEXT_HOP field of the UPDATE or the MP_REACH_NLRI next-hop).
Configurable	False

origin *keyword*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> origin <i>keyword</i>
Tree	origin
Description	The value of the ORIGIN path attribute
Options	<ul style="list-style-type: none">• igp• egp• incomplete
Configurable	False

originator-id (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> originator-id (<i>ipv4-address ipv6-address</i>)
Tree	originator-id
Description	The address in the ORIGINATOR_ID attribute added by a route reflector.
Configurable	False

unknown-attributes

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> unknown-attributes
Tree	unknown-attributes
Description	Container for unknown path attributes
Configurable	False

unknown-attribute [unknown-attr-index](#) *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> unknown-attributes unknown-attribute unknown-attr-index <i>number</i>
Tree	unknown-attribute
Description	
Configurable	False

unknown-attr-index *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> unknown-attributes unknown-attribute unknown-attr-index <i>number</i>
Description	RIB attribute unknown attribute index
Configurable	False

attr-len *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> unknown-attributes unknown-attribute unknown-attr-index <i>number</i> attr-len <i>number</i>
Tree	attr-len
Description	The length of the unknown path attribute
Configurable	False

attr-type *number*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> unknown-attributes unknown-attribute unknown-attr-index <i>number</i> attr-type <i>number</i>
Tree	attr-type
Description	The type code of the unknown path attribute
Configurable	False

extended *boolean*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index number unknown-attributes unknown-attribute unknown-attr-index <i>number</i> extended <i>boolean</i>
Tree	extended
Description	Set to true if the unknown path attribute has the extended length flag is set to 1.
Configurable	False

optional *boolean*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index number unknown-attributes unknown-attribute unknown-attr-index <i>number</i> optional <i>boolean</i>
Tree	optional
Description	Set to true if the unknown path attribute has the optional flag is set to 1.
Configurable	False

partial *boolean*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index number unknown-attributes unknown-attribute unknown-attr-index <i>number</i> partial <i>boolean</i>
Tree	partial
Description	Set to true if the unknown path attribute has the partial flag is set to 1.
Configurable	False

transitive *boolean*

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index number unknown-attributes unknown-attribute unknown-attr-index <i>number</i> transitive <i>boolean</i>
Tree	transitive
Description	Set to true if the unknown path attribute has the transitive flag is set to 1.
Configurable	False

ipv4-unicast

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast
Tree	ipv4-unicast
Description	Container for RIB state of IPv4-unicast routes.
Configurable	False

local-rib

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib
Tree	local-rib
Description	Container for local RIB, containing all imported routes from other protocols plus the post-import-policy version of all IPv4 routes learned from all BGP neighbors.
Configurable	False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Tree	routes
Description	List of IPv4 routes in the local RIB.
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

origin-protocol *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Description	If the route was imported from another protocol, this is the protocol name.
Options	<ul style="list-style-type: none">• static• aggregate• direct• bgp• host• isis• ospfv2• ospfv3• local• sdk
Configurable	False

attr-id *reference*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/bgp-rib/ attr-sets/attr-set/index
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Configurable	False

best-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> best-route <i>boolean</i>
Tree	best-route
Description	Set to true if the route is the BGP best path for the prefix.
Configurable	False

invalid-reason

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> invalid-reason
Tree	invalid-reason
Description	
Configurable	False

as-loop *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Configurable	False

cluster-loop *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Description	Indicates true if the BGP route has a cluster-list loop.
Configurable	False

next-hop-unresolved *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Configurable	False

rejected-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Description	Indicates true if the route was rejected by an import policy.
Configurable	False

last-modified *string*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> last-modified <i>string</i>
Tree	last-modified
Description	Time of the last modification of the route stored in the BGP RIB. For a route learned from a BGP neighbor the initial value is the same as last-updatereceived. If an import policy later changed some attribute of the route last-modified would be updated to reflect the time of this change.
Configurable	False

pending-delete *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> pending-delete <i>boolean</i>
Tree	pending-delete
Description	Set to true if the route is marked for deletion.
Configurable	False

stale-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> stale-route <i>boolean</i>
Tree	stale-route
Description	Set to true if the route is stale due to BGP graceful restart.
Configurable	False

tie-break-reason *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Options	<ul style="list-style-type: none">• unknown• none• origin• as-path-length• next-hop-cost• med• local-pref• aggregate• originator-id• cluster-list• aigp• rtm-pref• ebgp-route• peer-ip• invalid-route
Configurable	False

used-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> used-route <i>boolean</i>
Tree	used-route
Description	Indicates true if the route is being used for forwarding.
Configurable	False

valid-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> valid-route <i>boolean</i>
Tree	valid-route
Description	Indicates true if the route is valid.
Configurable	False

rib-in-out

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out
Tree	rib-in-out
Description	Container for BGP routes learned and advertised to BGP neighbors.
Configurable	False

rib-in-post

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post
Tree	rib-in-post
Description	Container for the post-import-policy version of BGP routes learned from BGP neighbors.
Configurable	False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	routes
Description	List of IPv4 routes
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

attr-id *reference*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Configurable	False

best-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) best-route <i>boolean</i>
Tree	best-route
Description	Set to true if the route is the BGP best path for the prefix.
Configurable	False

invalid-reason

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason
Tree	invalid-reason
Description	
Configurable	False

as-loop *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Configurable	False

cluster-loop *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Description	Indicates true if the BGP route has a cluster-list loop.
Configurable	False

next-hop-unresolved *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Configurable	False

rejected-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Description	Indicates true if the route was rejected by an import policy.
Configurable	False

last-modified *string*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) last-modified <i>string</i>
Tree	last-modified
Description	Time of the last modification of the route stored in the BGP RIB. For a route learned from a BGP neighbor the initial value is the same as last-updatereceived. If an import policy later changed some attribute of the route last-modified would be updated to reflect the time of this change.
Configurable	False

pending-delete *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) pending-delete <i>boolean</i>
Tree	pending-delete
Description	Set to true if the route is marked for deletion.
Configurable	False

stale-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) stale-route <i>boolean</i>
Tree	stale-route
Description	Set to true if the route is stale due to BGP graceful restart.
Configurable	False

tie-break-reason *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Options	<ul style="list-style-type: none">• unknown• none• origin• as-path-length• next-hop-cost• med

- local-pref
- aggregate
- originator-id
- cluster-list
- aigp
- rtm-pref
- ebgp-route
- peer-ip
- invalid-route

Configurable False

used-route *boolean*

Context **network-instance name** *string* **bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **used-route** *boolean*

Tree **used-route**

Description Indicates true if the route is being used for forwarding.

Configurable False

valid-route *boolean*

Context **network-instance name** *string* **bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **valid-route** *boolean*

Tree **valid-route**

Description Indicates true if the route is valid.

Configurable False

rib-in-pre

Context **network-instance name** *string* **bgp-rib ipv4-unicast rib-in-out rib-in-pre**

Tree **rib-in-pre**

Description Container for the pre-import-policy version of BGP routes learned from BGP neighbors.

Configurable False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	routes
Description	List of IPv4 routes.
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

attr-id *reference*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Configurable	False

rib-out-post

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post
Tree	rib-out-post
Description	Container for the post-export-policy version of BGP routes advertised to BGP neighbors.
Configurable	False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	routes
Description	List of IPv4 routes.
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

attr-id *reference*

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Configurable	False

ipv6-unicast

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast
Tree	ipv6-unicast
Description	Container for RIB state of IPv6-unicast routes.
Configurable	False

local-rib

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib
Tree	local-rib
Description	Container for local RIB, containing all imported routes from other protocols plus the post-import-policy version of all IPv4 routes learned from all BGP neighbors.
Configurable	False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Tree	routes
Description	List of IPv6 routes in the local RIB.
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

origin-protocol *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i>
Description	If the route was imported from another protocol, this is the protocol name.
Options	<ul style="list-style-type: none">• static• aggregate• direct

- bgp
- host
- isis
- ospfv2
- ospfv3
- local
- sdk

Configurable False

attr-id *reference*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword* **attr-id** *reference*

Tree **attr-id**

Description Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index

Reference **network-instance name** *string* **bgp-rib attr-sets attr-set attr-set-type** *keyword* **index** *number*

Configurable False

best-route *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword* **best-route** *boolean*

Tree **best-route**

Description Set to true if the route is the BGP best path for the prefix.

Configurable False

invalid-reason

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword* **invalid-reason**

Tree **invalid-reason**

Description

Configurable False

as-loop *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*
invalid-reason as-loop *boolean*

Tree **as-loop**

Description Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.

Configurable False

cluster-loop *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*
invalid-reason cluster-loop *boolean*

Tree **cluster-loop**

Description Indicates true if the BGP route has a cluster-list loop.

Configurable False

next-hop-unresolved *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*
invalid-reason next-hop-unresolved *boolean*

Tree **next-hop-unresolved**

Description Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.

Configurable False

rejected-route *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword*
invalid-reason rejected-route *boolean*

Tree **rejected-route**

Description Indicates true if the route was rejected by an import policy.

Configurable False

last-modified *string*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> last-modified <i>string</i>
Tree	last-modified
Description	Time of the last modification of the route stored in the BGP RIB. For a route learned from a BGP neighbor the initial value is the same as last-updatereceived. If an import policy later changed some attribute of the route last-modified would be updated to reflect the time of this change.
Configurable	False

pending-delete *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> pending-delete <i>boolean</i>
Tree	pending-delete
Description	Set to true if the route is marked for deletion.
Configurable	False

stale-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> stale-route <i>boolean</i>
Tree	stale-route
Description	Set to true if the route is stale due to BGP graceful restart.
Configurable	False

tie-break-reason *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) origin-protocol <i>keyword</i> tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Options	<ul style="list-style-type: none">• unknown• none• origin

- as-path-length
- next-hop-cost
- med
- local-pref
- aggregate
- originator-id
- cluster-list
- aigp
- rtm-pref
- ebgp-route
- peer-ip
- invalid-route

Configurable False

used-route *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword* **used-route** *boolean*

Tree **used-route**

Description Indicates true if the route is being used for forwarding.

Configurable False

valid-route *boolean*

Context **network-instance name** *string* **bgp-rib ipv6-unicast local-rib routes prefix** (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*) **origin-protocol** *keyword* **valid-route** *boolean*

Tree **valid-route**

Description Indicates true if the route is valid.

Configurable False

rib-in-out

Context **network-instance name** *string* **bgp-rib ipv6-unicast rib-in-out**

Tree **rib-in-out**

Description Container for BGP routes learned and advertised to BGP neighbors.

Configurable False

rib-in-post

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post
Tree	rib-in-post
Description	Container for the post-import-policy version of BGP routes learned from BGP neighbors.
Configurable	False

routes [prefix](#) (*ipv4-prefix | ipv6-prefix*) [neighbor](#) (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	routes
Description	List of IPv6 routes
Configurable	False

[prefix](#) (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	
Configurable	False

[neighbor](#) (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

[attr-id](#) *reference*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Configurable	False

best-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) best-route <i>boolean</i>
Tree	best-route
Description	Set to true if the route is the BGP best path for the prefix.
Configurable	False

invalid-reason

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason
Tree	invalid-reason
Description	
Configurable	False

as-loop *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Configurable	False

cluster-loop *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Description	Indicates true if the BGP route has a cluster-list loop.
Configurable	False

next-hop-unresolved *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Configurable	False

rejected-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Description	Indicates true if the route was rejected by an import policy.
Configurable	False

last-modified *string*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) last-modified <i>string</i>
Tree	last-modified
Description	Time of the last modification of the route stored in the BGP RIB. For a route learned from a BGP neighbor the initial value is the same as last-updatereceived. If an import policy later changed some attribute of the route last-modified would be updated to reflect the time of this change.
Configurable	False

pending-delete *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) pending-delete <i>boolean</i>
Tree	pending-delete
Description	Set to true if the route is marked for deletion.
Configurable	False

stale-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) stale-route <i>boolean</i>
Tree	stale-route
Description	Set to true if the route is stale due to BGP graceful restart.
Configurable	False

tie-break-reason *keyword*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Options	<ul style="list-style-type: none">• unknown• none• origin• as-path-length• next-hop-cost• med• local-pref• aggregate• originator-id• cluster-list• aigp• rtm-pref• ebgp-route• peer-ip• invalid-route
Configurable	False

used-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) used-route <i>boolean</i>
Tree	used-route
Description	Indicates true if the route is being used for forwarding.
Configurable	False

valid-route *boolean*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) valid-route <i>boolean</i>
Tree	valid-route
Description	Indicates true if the route is valid.
Configurable	False

rib-in-pre

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre
Tree	rib-in-pre
Description	Container for the pre-import-policy version of BGP routes learned from BGP neighbors.
Configurable	False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	routes
Description	List of IPv6 routes.
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

attr-id *reference*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index number
Configurable	False

rib-out-post

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-out-post
Tree	rib-out-post
Description	Container for the post-export-policy version of BGP routes advertised to BGP neighbors.
Configurable	False

routes prefix (*ipv4-prefix | ipv6-prefix*) **neighbor** (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	routes
Description	List of IPv6 routes.
Configurable	False

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	
Configurable	False

neighbor (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix ipv6-prefix</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Configurable	False

attr-id *reference*

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-out-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) attr-id <i>reference</i>
Tree	attr-id
Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i>
Configurable	False

bridge-table

Context	network-instance name <i>string</i> bridge-table
Tree	bridge-table
Description	Builds a bridge table
Configurable	True

discard-unknown-dest-mac *boolean*

Context	network-instance name <i>string</i> bridge-table discard-unknown-dest-mac <i>boolean</i>
Tree	discard-unknown-dest-mac
Description	To discard unknown destination macs
Default	false
Configurable	True

mac-duplication

Context	network-instance name <i>string</i> bridge-table mac-duplication
Tree	mac-duplication
Description	Configuration of the MAC duplication procedures.
Configurable	True

action *keyword*

Context	network-instance name <i>string</i> bridge-table mac-duplication action <i>keyword</i>
Tree	action
Description	Action to take on the subinterface whose action is use-net-instance-action, upon detecting one or more mac addresses as duplicate In particular:

- Oper-down: if configured, upon detecting a duplicate mac on the subinterface, the subinterface will be brought oper-down.
- Blackhole: upon detecting a duplicate mac on the subinterface, the mac will be blackholed. Any frame received on this or any other subinterface with MAC SA matching a blackhole mac will be discarded.
- Stop-learning: this is the default action, compliant with RFC7432. Upon detecting a duplicate mac on the subinterface, the mac will not be relearned anymore on this or any subinterface.

Default stop-learning

Options

- stop-learning
- blackhole
- oper-down

Configurable True

admin-state *keyword*

Context **network-instance name** *string* **bridge-table mac-duplication admin-state** *keyword*

Tree **admin-state**

Description Configurable state of the mac-duplication procedures. Mac-duplication detects duplicate macs that move between different subinterfaces or a subinterface and an evpn destination.

Default enable

Options

- enable
- disable

Configurable True

duplicate-entries

Context **network-instance name** *string* **bridge-table mac-duplication duplicate-entries**

Tree **duplicate-entries**

Description

Configurable False

mac address *string*

Context **network-instance name** *string* **bridge-table mac-duplication duplicate-entries mac address** *string*

Tree **mac**

Description macs duplicate on the bridging instance

Configurable False

address *string*

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Description	
Configurable	False

destination *string*

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> destination <i>string</i>
Tree	destination
Description	the name of the destination the duplicate mac is installed against in the fdb.
Configurable	False

destination-index *number*

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> destination-index <i>number</i>
Tree	destination-index
Description	A system-wide unique identifier of a subinterface object (system allocated).
Configurable	False

destination-type *keyword*

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> destination-type <i>keyword</i>
Tree	destination-type
Description	the type of the destination the duplicate mac is installed against in the fdb.
Options	<ul style="list-style-type: none">• sub-interface• blackhole• irb-interface
Configurable	False

dup-detect-time *string*

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> dup-detect-time <i>string</i>
Tree	dup-detect-time
Description	The date and time when the mac was declared duplicate
Configurable	False

hold-down-time-remaining *number*

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> hold-down-time-remaining <i>number</i>
Tree	hold-down-time-remaining
Description	remaining hold down time for duplicate mac
Units	seconds
Configurable	False

hold-down-time *number*

Context	network-instance name <i>string</i> bridge-table mac-duplication hold-down-time <i>number</i>
Tree	hold-down-time
Description	Time to wait from the moment a mac is declared duplicate to the mac is flushed from the bridge table. When the duplicate mac is flushed, the monitoring process for the mac is restarted.
Range	2 to 600
Default	10
Units	seconds
Configurable	True

monitoring-window *number*

Context	network-instance name <i>string</i> bridge-table mac-duplication monitoring-window <i>number</i>
Tree	monitoring-window
Description	Monitoring window for detecting duplication on a given mac address. A mac is declared as duplicate if it exceed the num-moves within the monitoring-window.
Range	1 to 15
Default	3
Units	minutes
Configurable	True

num-moves *number*

Context	network-instance name <i>string</i> bridge-table mac-duplication num-moves <i>number</i>
Tree	num-moves
Description	Number of moves a mac is allowed within the monitoring-window, before it is declared duplicate.
Range	3 to 10
Default	5
Configurable	True

mac-learning

Context	network-instance name <i>string</i> bridge-table mac-learning
Tree	mac-learning
Description	
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> bridge-table mac-learning admin-state <i>keyword</i>
Tree	admin-state
Description	Configurable state of the learning procedures for dynamic mac addresses. If disabled, no mac addresses will be learned.
Default	enable
Options	<ul style="list-style-type: none">enable

	<ul style="list-style-type: none">• disable
Configurable	True

aging

Context	network-instance name <i>string</i> bridge-table mac-learning aging
Tree	aging
Description	
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> bridge-table mac-learning aging admin-state <i>keyword</i>
Tree	admin-state
Description	Configurable state of the aging for the dynamic mac entries in the bridge table. If disabled, dynamically learned mac entries will be programmed in the bridge table until the network instance is disabled.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

age-time *number*

Context	network-instance name <i>string</i> bridge-table mac-learning aging age-time <i>number</i>
Tree	age-time
Description	Configurable aging time for dynamically learned mac addresses
Range	60 to 86400
Default	300
Configurable	True

learnt-entries

Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries
Tree	learnt-entries
Description	Learnt entries
Configurable	False

mac address *string*

Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i>
Tree	mac
Description	Macs learnt on the bridging instance
Configurable	False

address *string*

Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i>
Description	
Configurable	False

aging (*number | keyword*)

Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i> aging (<i>number keyword</i>)
Tree	aging
Description	Remaining age time for learnt macs
Units	seconds
Options	<ul style="list-style-type: none">disabled
Configurable	False

destination *string*

Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i> destination <i>string</i>
Tree	destination
Description	The name of the subinterface where the mac is learnt against.
Configurable	False

last-update *string*

Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address string last-update <i>string</i>
Tree	last-update
Description	The date and time of the last update of this learnt mac
Configurable	False

mac-relearn-only *boolean*

Context	network-instance name <i>string</i> bridge-table mac-learning mac-relearn-only <i>boolean</i>
Tree	mac-relearn-only
Description	The value of this leaf indicates that network-instance will not learn any new mac addresses, but will relearn any that are already programmed
Default	true
Configurable	False

oper-mac-learning *keyword*

Context	network-instance name <i>string</i> bridge-table mac-learning oper-mac-learning <i>keyword</i>
Tree	oper-mac-learning
Description	The operational state of mac-learning on this network instance.
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading

Component is currently being upgraded

Configurable False

oper-mac-learning-disabled-reason *keyword*

Context [network-instance name](#) *string* [bridge-table mac-learning oper-mac-learning-disabled-reason](#) *keyword*

Tree [oper-mac-learning-disabled-reason](#)

Description The reason for the mac-learning being disabled on this network instance

Options

- admin-disabled

Configurable False

mac-limit

Context [network-instance name](#) *string* [bridge-table mac-limit](#)

Tree [mac-limit](#)

Description Bridge Table size and thresholds.

Configurable True

maximum-entries *number*

Context [network-instance name](#) *string* [bridge-table mac-limit maximum-entries](#) *number*

Tree [maximum-entries](#)

Description Maximum number of mac addresses allowed in the bridge-table.

Range 1 to 8192

Default 250

Configurable True

warning-threshold-pct *number*

Context [network-instance name](#) *string* [bridge-table mac-limit warning-threshold-pct](#) *number*

Tree [warning-threshold-pct](#)

Description Percentage of the configured max-number-macs over which a warning is triggered. The warning message is cleared when the percentage drops below the configured percentage minus 5%

Range 6 to 100

Default 95

Configurable True

mac-table

Context	network-instance name <i>string</i> bridge-table mac-table
Tree	mac-table
Description	
Configurable	False

mac address *string*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i>
Tree	mac
Description	macs learnt on the bridging instance
Configurable	False

address *string*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i>
Description	
Configurable	False

destination *string*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> destination <i>string</i>
Tree	destination
Description	the name of the destination where the mac is programmed against.
Configurable	False

destination-index *number*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> destination-index <i>number</i>
Tree	destination-index
Description	A system-wide unique identifier of a subinterface object (system allocated).
Configurable	False

destination-type *keyword*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> destination-type <i>keyword</i>
Tree	destination-type
Description	the type of the destination the mac installed against in the fdb.
Options	<ul style="list-style-type: none">• sub-interface• blackhole• irb-interface
Configurable	False

failed-slots *number*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> failed-slots <i>number</i>
Tree	failed-slots
Description	The list of slot IDs corresponding to the linecards that did not successfully program the mac
Range	1 to 8
Configurable	False

last-update *string*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> last-update <i>string</i>
Tree	last-update
Description	The date and time of the last update of this mac
Configurable	False

not-programmed-reason *keyword*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> not-programmed-reason <i>keyword</i>
Tree	not-programmed-reason
Description	The reason why the mac is not programmed
Options	<ul style="list-style-type: none">• mac-limit
Configurable	False

type *keyword*

Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> type <i>keyword</i>
Tree	type
Description	the type of the mac installed in the fib.
Options	<ul style="list-style-type: none">• static• duplicate• learnt• irb-interface
Configurable	False

static-mac

Context	network-instance name <i>string</i> bridge-table static-mac
Tree	static-mac
Description	
Configurable	True

mac address *string*

Context	network-instance name <i>string</i> bridge-table static-mac mac address <i>string</i>
Tree	mac
Description	static macs configured on the bridging instance
Configurable	True

address *string*

Context	network-instance name <i>string</i> bridge-table static-mac mac address <i>string</i>
Description	
Configurable	True

destination (*keyword | reference*)

Context	network-instance name <i>string</i> bridge-table static-mac mac address <i>string</i> destination (<i>keyword reference</i>)
Tree	destination
Description	the destination where the mac is programmed against.
Options	<ul style="list-style-type: none">• blackhole
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True

statistics

Context	network-instance name <i>string</i> bridge-table statistics
Tree	statistics
Description	Display statistics
Configurable	False

active-entries *number*

Context	network-instance name <i>string</i> bridge-table statistics active-entries <i>number</i>
Tree	active-entries
Description	The total number of entries that are active in the mac-table.
Default	0
Configurable	False

mac-type **type** *keyword*

Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i>
Tree	mac-type
Description	the type of the mac installed in the fib.
Configurable	False

type *keyword*

Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i>
Description	
Options	<ul style="list-style-type: none">• static• duplicate

	<ul style="list-style-type: none">• learnt• irb-interface
Configurable	False

active-entries *number*

Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i> active-entries <i>number</i>
Tree	active-entries
Description	The total number of entries of this type that are active in the mac-table.
Default	0
Configurable	False

total-entries *number*

Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i> total-entries <i>number</i>
Tree	total-entries
Description	The total number of macs of this type , active and inactive, that are present in the mac-table.
Default	0
Configurable	False

total-entries *number*

Context	network-instance name <i>string</i> bridge-table statistics total-entries <i>number</i>
Tree	total-entries
Description	The total number of macs, active and inactive, that are present in the mac-table.
Default	0
Configurable	False

description *string*

Context	network-instance name <i>string</i> description <i>string</i>
Tree	description
Description	A user-entered description of this network instance.
String Length	1 to 255
Configurable	True

icmp

Context	network-instance name <i>string</i> icmp
Tree	icmp
Description	
Configurable	True

statistics

Context	network-instance name <i>string</i> icmp statistics
Tree	statistics
Description	ICMP version 4 statistics
Configurable	False

last-clear *string*

Context	network-instance name <i>string</i> icmp statistics last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the interface counters were cleared.
Configurable	False

total

Context	network-instance name <i>string</i> icmp statistics total
Tree	total
Description	Aggregate statistics, counting all ICMP message types
Configurable	False

in-error-packets *number*

Context	network-instance name <i>string</i> icmp statistics total in-error-packets <i>number</i>
Tree	in-error-packets
Description	The number of ICMPv4 messages that the network instance received and extracted successfully to the CPM but when they arrived they were determined to have ICMP-specific errors (bad ICMP checksums, bad length, etc.)
Default	0
Configurable	False

in-packets *number*

Context	network-instance name <i>string icmp statistics total in-packets number</i>
Tree	in-packets
Description	The total number of ICMPv4 messages that the network instance received and extracted successfully to the CPM. Note that this counter includes all those counted by in-error-packets.
Default	0
Configurable	False

out-error-packets *number*

Context	network-instance name <i>string icmp statistics total out-error-packets number</i>
Tree	out-error-packets
Description	The number of ICMPv4 messages that this network instance did not send due to issues such as fragmentation required but not supported.
Default	0
Configurable	False

out-packets *number*

Context	network-instance name <i>string icmp statistics total out-packets number</i>
Tree	out-packets
Description	The total number of ICMPv4 messages that the network instance attempted to send. Note that this counter includes all those counted by out-error-packets.
Default	0
Configurable	False

type name *keyword*

Context	network-instance name <i>string icmp statistics type name keyword</i>
Tree	type
Description	
Configurable	False

name *keyword*

Context	network-instance name <i>string icmp statistics type name keyword</i>
Description	
Options	<ul style="list-style-type: none">• echo-reply

- dest-unreachable
- redirect
- echo
- rtr-advertisement
- rtr-selection
- time-exceeded
- param-problem
- timestamp
- timestamp-reply

Configurable False

in-packets *number*

Context **network-instance name** *string icmp statistics type name keyword in-packets number*
Tree **in-packets**
Description The total number of ICMPv4 messages of this type that the network instance received and extracted successfully to the CPM.
Default 0
Configurable False

out-packets *number*

Context **network-instance name** *string icmp statistics type name keyword out-packets number*
Tree **out-packets**
Description The total number of ICMPv4 messages of this type that the network instance attempted to send.
Default 0
Configurable False

icmp6

Context **network-instance name** *string icmp6*
Tree **icmp6**
Description
Configurable True

statistics

Context	network-instance name <i>string</i> icmp6 statistics
Tree	statistics
Description	ICMP version 6 statistics
Configurable	False

last-clear *string*

Context	network-instance name <i>string</i> icmp6 statistics last-clear <i>string</i>
Tree	last-clear
Description	Timestamp of the last time the interface counters were cleared.
Configurable	False

total

Context	network-instance name <i>string</i> icmp6 statistics total
Tree	total
Description	Aggregate statistics, counting all ICMP message types
Configurable	False

in-error-packets *number*

Context	network-instance name <i>string</i> icmp6 statistics total in-error-packets <i>number</i>
Tree	in-error-packets
Description	The number of ICMPv6 messages that the network instance received and extracted successfully to the CPM but when they arrived they were determined to have ICMP-specific errors (bad ICMP checksums, bad length, etc.)
Default	0
Configurable	False

in-packets *number*

Context	network-instance name <i>string</i> icmp6 statistics total in-packets <i>number</i>
Tree	in-packets
Description	The total number of ICMPv6 messages that the network instance received and extracted successfully to the CPM. Note that this counter includes all those counted by in-error-packets.
Default	0
Configurable	False

out-error-packets *number*

Context	network-instance name <i>string</i> icmp6 statistics total out-error-packets <i>number</i>
Tree	out-error-packets
Description	The number of ICMPv6 messages that this network instance did not send due to issues such as fragmentation required but not supported.
Default	0
Configurable	False

out-packets *number*

Context	network-instance name <i>string</i> icmp6 statistics total out-packets <i>number</i>
Tree	out-packets
Description	The total number of ICMPv6 messages that the network instance attempted to send. Note that this counter includes all those counted by out-error-packets.
Default	0
Configurable	False

type name *keyword*

Context	network-instance name <i>string</i> icmp6 statistics type name <i>keyword</i>
Tree	type
Description	
Configurable	False

name *keyword*

Context	network-instance name <i>string</i> icmp6 statistics type name <i>keyword</i>
Description	
Options	<ul style="list-style-type: none">• dest-unreachable• packet-too-big• time-exceeded• param-problem• echo-request• echo-reply• rtr-solicitation• rtr-advertisement• nbr-solicitation• nbr-advertisement

Configurable • redirect
False

in-packets *number*

Context **network-instance name** *string icmp6 statistics type name* *keyword in-packets* *number*
Tree **in-packets**
Description The total number of ICMPv6 messages of this type that the network instance received and extracted successfully to the CPM.
Default 0
Configurable False

out-packets *number*

Context **network-instance name** *string icmp6 statistics type name* *keyword out-packets* *number*
Tree **out-packets**
Description The total number of ICMPv6 messages of this type that the network instance attempted to send.
Default 0
Configurable False

interface name *string*

Context **network-instance name** *string interface name* *string*
Tree **interface**
Description List of subinterfaces used by this network-instance
Configurable True

name *string*

Context **network-instance name** *string interface name* *string*
Description Identifier of sub-interface used in this network-instance
String Length 3 to 24
Configurable True

index number *number*

Context	network-instance name <i>string</i> interface name <i>string</i> index <i>number</i>
Tree	index
Description	network instance allocated sub interface index
Default	0
Configurable	False

mac-relearn-only *boolean*

Context	network-instance name <i>string</i> interface name <i>string</i> mac-relearn-only <i>boolean</i>
Tree	mac-relearn-only
Description	The value of this leaf indicates that the interface will not learn any new mac addresses, but will relearn any that are already programmed
Default	true
Configurable	False

oper-down-reason *keyword*

Context	network-instance name <i>string</i> interface name <i>string</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Description	The reason for the interface being down in the network-instance
Options	<ul style="list-style-type: none">• ip-addr-missing• ip-addr-overlap• subif-down• net-inst-down• vrf-type-mismatch• mac-dup-detected• associated-mac-vrf-down• mac-vrf-association-missing• associated-ip-vrf-down
Configurable	False

oper-mac-learning *keyword*

Context	network-instance name <i>string</i> interface name <i>string</i> oper-mac-learning <i>keyword</i>
Tree	oper-mac-learning
Description	The operational state of mac-learning on this subinterface.
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

oper-mac-learning-disabled-reason *keyword*

Context	network-instance name <i>string</i> interface name <i>string</i> oper-mac-learning-disabled-reason <i>keyword</i>
Tree	oper-mac-learning-disabled-reason
Description	The reason for the mac-learning being disabled on this interface
Options	<ul style="list-style-type: none">• routed• admin-disabled• mac-dup-detected
Configurable	False

oper-state *keyword*

Context	network-instance name <i>string</i> interface name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of this subinterface.
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

ip-forwarding

Context	network-instance name <i>string</i> ip-forwarding
Tree	ip-forwarding
Description	Forwarding options that apply to the entire network instance.
Configurable	True

receive-ipv4-check *boolean*

Context	network-instance name <i>string</i> ip-forwarding receive-ipv4-check <i>boolean</i>
Tree	receive-ipv4-check
Description	If set to true then the following check is done on every subinterface of the network-instance: if an IPv4 packet is received on a subinterface and the IPv4 oper-status of this subinterface is down the packet is discarded. If this leaf is set to false then received IPv4 packets are accepted on all subinterfaces of the network-instance that are up, even if they do not have any IPv4 addresses.
Default	true
Configurable	True

receive-ipv6-check *boolean*

Context	network-instance name <i>string</i> ip-forwarding receive-ipv6-check <i>boolean</i>
Tree	receive-ipv6-check
Description	If set to true then the following check is done on every subinterface of the network-instance: if an IPv6 packet is received on a subinterface and the IPv6 oper-status of this subinterface is down the packet is discarded. If this leaf is set to false then received IPv6 packets are accepted on all subinterfaces of the network-instance that are up, even if they do not have any IPv6 addresses.
Default	true
Configurable	True

ip-load-balancing

Context	network-instance name <i>string</i> ip-load-balancing
Tree	ip-load-balancing
Description	Container for IP load-balancing options that are specific to the network-instance
Configurable	True

resilient-hash-prefix **ip-prefix** (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	resilient-hash-prefix
Description	List of IPv4 and IPv6 prefixes which should be programmed for resilient ECMP hashing.
Configurable	True

ip-prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>)
Description	IPv4 or IPv6 prefix. Active routes in the FIB that exactly match this prefix or that are longer matches of this prefix are provided with resilient-hash programming.
Configurable	True

hash-buckets-per-path *number*

Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>) hash-buckets-per-path <i>number</i>
Tree	hash-buckets-per-path
Description	The number of times each next-hop is repeated in the fill pattern if there are max-paths ECMP next-hops A larger number consumes more resources but provides more granularity when flows need to be moved. Note that hash-buckets-per-path * max-paths must be less than or equal to 128.
Range	1 to 32
Default	1
Configurable	True

max-paths *number*

Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>) max-paths <i>number</i>
Tree	max-paths
Description	The maximum number of ECMP next-hops per route associated with the resilient-hash prefix If a matching route has more than this number of ECMP next-hops only the first N are used, where N is the value of this parameter. Note that hash-buckets-per-path * max-paths must be less than or equal to 128.
Range	1 to 64
Default	1
Configurable	True

mpls

Context	network-instance name <i>string</i> mpls
Tree	mpls
Description	
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> mpls admin-state <i>keyword</i>
Tree	admin-state
Description	Used to administratively enable or disable MPLS. When MPLS is enabled, MPLS packets can be sent and received on any subinterface assigned to the base network-instance. When MPLS is disabled, MPLS packets are discarded if received or sent on any subinterface of the base network-instance.
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

static-mpls-entry [top-label](#) (*number | keyword*)

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>)
Tree	static-mpls-entry
Description	
Configurable	True

[top-label](#) (*number | keyword*)

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>)
Description	A received MPLS packet, received on any subinterface, matches this static entry if its top label stack entry contains the label value specified by this leaf.
Range	16 to 1048575
Options	<ul style="list-style-type: none">• IMPLICIT_NULL assigned by local LSR but not carried in packets
Configurable	True

collect-stats *boolean*

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>) collect-stats <i>boolean</i>
Tree	collect-stats
Description	When set to true, stats resources are used to count the number of incoming packets matching the top label value of this static MPLS route
Default	false
Configurable	True

installed *boolean*

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>) installed <i>boolean</i>
Tree	installed
Description	Indicates whether the MPLS route entry was programmed in the data path
Configurable	False

next-hop-group *reference*

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>) next-hop-group <i>reference</i>
Tree	next-hop-group
Description	
Reference	network-instance name <i>string</i> next-hop-groups group name <i>string</i>
Configurable	True

operation *keyword*

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>) operation <i>keyword</i>
Tree	operation
Description	Operation of MPLS labels in the label stack
Default	swap
Options	<ul style="list-style-type: none">• pop• swap
Configurable	True

origin-protocol *identityref*

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>) origin-protocol <i>identityref</i>
Tree	origin-protocol
Description	The protocol from which the MPLS route entry was learned.
Options	<ul style="list-style-type: none">• mpls-static Locally configured static route• mpls-sdk MPLS label entry added by an agent application using the SDK
Configurable	False

preference *number*

Context	network-instance name <i>string</i> mpls static-mpls-entry top-label (<i>number keyword</i>) preference <i>number</i>
Tree	preference
Description	MPLS route preference with lower values indicating a higher degree of preference
Range	0 to 255
Default	5
Configurable	True

ttl-propagation *boolean*

Context	network-instance name <i>string</i> mpls ttl-propagation <i>boolean</i>
Tree	ttl-propagation
Description	Propagate TTL between IP and MPLS
Default	false
Configurable	True

mtu

Context	network-instance name <i>string</i> mtu
Tree	mtu
Description	Top-level container for configuration and state data related to network-instance MTU
Configurable	True

path-mtu-discovery *boolean*

Context	network-instance name <i>string</i> mtu path-mtu-discovery <i>boolean</i>
Tree	path-mtu-discovery
Description	<p>Enables or disables path MTU discovery in this network-instance</p> <p>This is controlled via the kernel <code>ip_no_pmtu_disc</code> option. Path MTU discovery (PMTUD) is a standardized technique in networking for determining the MTU size on the network path between two hosts, usually with the goal of avoiding IP fragmentation.</p> <p>For IPv4 packets, Path MTU discovery works by setting the Don't Fragment (DF) flag bit in the IP headers of outgoing packets. Then, any device along the path whose MTU is smaller than the packet will drop it, and send back an Internet Control Message Protocol (ICMP) Fragmentation Needed (Type 3, Code 4) message containing its MTU, allowing the source host to reduce its Path MTU appropriately. The process is repeated until the MTU is small enough to traverse the entire path without fragmentation.</p>
Default	true
Configurable	True

next-hop-groups

Context	network-instance name <i>string</i> next-hop-groups
Tree	next-hop-groups
Description	
Configurable	True

group name *string*

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i>
Tree	group
Description	Specifies the next hop group.
Configurable	True

name *string*

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i>
Description	Specifies the next hop group name
String Length	1 to 255
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Used to enable or disable a next-hop group
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

blackhole

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> blackhole
Tree	blackhole
Description	
Configurable	True

generate-icmp *boolean*

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> blackhole generate-icmp <i>boolean</i>
Tree	generate-icmp
Description	When set to true the router generates ICMP unreachable messages for the dropped packets
Default	false
Configurable	True

nexthop index *number*

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index <i>number</i>
Tree	nexthop
Description	
Configurable	True
Max. Elements	128

index number

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number
Description	Numerical index of the next-hop member
Configurable	True

admin-state keyword

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number admin-state <i>keyword</i>
Tree	admin-state
Description	Used to enable or disable a particular next-hop
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

ip-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number ip-address (<i>ipv4-address ipv6-address</i>)
Tree	ip-address
Description	The next-hop IPv4 or IPv6 address
Configurable	True

pushed-mpls-label-stack (*number | keyword*)

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number pushed-mpls-label-stack (<i>number keyword</i>)
Tree	pushed-mpls-label-stack
Description	A list of MPLS labels to push onto the packet when forwarding to this particular next-hop Default is none/empty. Pushing an MPLS label stack is not supported unless the resolve flag is set to false.
Range	16 to 1048575
Options	<ul style="list-style-type: none">• IMPLICIT_NULL assigned by local LSR but not carried in packets
Configurable	True
Max. Elements	1

resolve *boolean*

Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index <i>number</i> resolve <i>boolean</i>
Tree	resolve
Description	When set to true, the router is allowed to use any route to resolve the nexthop address to an outgoing interface When set to false the router is only allowed to use a local route to resolve the next-hop address.
Default	true
Configurable	True

oper-mac-vrf-mtu *number*

Context	network-instance name <i>string</i> oper-mac-vrf-mtu <i>number</i>
Tree	oper-mac-vrf-mtu
Description	Operational I2-mtu of the mac-vrf network-instance. Calculated as the lowest I2-mtu of the bridged subinterfaces associated to the mac-vrf, minus the vlan tags associated to that subinterface (lowest mtu subinterface). When the mac-vrf has an associated irb subinterface, if the configured irb ip-mtu exceeds the oper-mac-vrf-mtu minus 14 bytes (Ethernet header), then the irb subinterface will remain operationally down. The oper-mac-vrf-mtu is only available in mac-vrf network-instances.
Range	1492 to 9500
Units	bytes
Configurable	False

oper-state *keyword*

Context	network-instance name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Description	This leaf contains the operational state of the network instance.
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading

- Component is downloading image into memory
- booting
Component is booting downloaded image
- starting
Component image operational, application processes starting
- failed
Component or process has failed
- synchronizing
Component is currently being synchronized
- upgrading
Component is currently being upgraded

Configurable False

protocols

Context [network-instance name](#) *string* [protocols](#)

Tree [protocols](#)

Description The routing protocols that are enabled for this network-instance.

Configurable True

bgp

Context [network-instance name](#) *string* [protocols](#) [bgp](#)

Tree [bgp](#)

Description BGP

Configurable True

admin-state *keyword*

Context [network-instance name](#) *string* [protocols](#) [bgp](#) [admin-state](#) *keyword*

Tree [admin-state](#)

Description Administratively enable or disable the entire BGP instance

Disable causes all BGP sessions to be taken down immediately, even if admin-state at the group or neighbor level of some of these sessions is still set as enable.

Default enable

Options

- enable
- disable

Configurable True

as-path-options

Context	network-instance name <i>string</i> protocols bgp as-path-options
Tree	as-path-options
Description	Options for handling the AS_PATH in received BGP routes
Configurable	True

allow-own-as *number*

Context	network-instance name <i>string</i> protocols bgp as-path-options allow-own-as <i>number</i>
Tree	allow-own-as
Description	The maximum number of times the global AS number or a local AS number of the BGP instance can appear in any received AS_PATH before it is considered a loop and considered invalid
Default	0
Configurable	True

remove-private-as

Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as
Tree	remove-private-as
Description	Container with options for removing private AS numbers (2-byte and 4-byte) from the advertised AS path towards all peers
Configurable	True

ignore-peer-as *boolean*

Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as ignore-peer-as <i>boolean</i>
Tree	ignore-peer-as
Description	If set to true then do not delete or replace a private AS number that is the same as the peer AS number
Default	false
Configurable	True

leading-only *boolean*

Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as leading-only <i>boolean</i>
Tree	leading-only
Description	If set to true then only delete or replace private AS numbers that appear before the first occurrence of a non-private ASN in the sequence of most recent ASNs in the AS path
Default	false
Configurable	True

mode *keyword*

Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as mode <i>keyword</i>
Tree	mode
Description	The method by which private AS numbers are removed from the advertised AS_PATH attribute
Default	disabled
Options	<ul style="list-style-type: none">• disabled Do not strip or replace any private AS numbers• delete Delete private AS numbers, shortening the AS path• replace Replace private AS numbers with the local AS number used towards the peer, maintaining the AS path length
Configurable	True

authentication

Context	network-instance name <i>string</i> protocols bgp authentication
Tree	authentication
Description	Container with authentication options that apply to all peers of the BGP instance
Configurable	True

keychain *reference*

Context	network-instance name <i>string</i> protocols bgp authentication keychain <i>reference</i>
Tree	keychain
Description	Reference to a keychain. The keychain type must be tcp-md5 or tcp-ao.
Reference	system authentication keychain name <i>string</i>
Configurable	True

autonomous-system *number*

Context	network-instance name <i>string</i> protocols bgp autonomous-system <i>number</i>
Tree	autonomous-system
Description	The global AS number of the BGP instance Values greater than 65535 must be entered in ASPLAIN format.
Range	1 to 4294967295
Configurable	True

convergence

Context	network-instance name <i>string</i> protocols bgp convergence
Tree	convergence
Description	Options for configuring address family independent BGP convergence parameters
Configurable	True

min-wait-to-advertise *number*

Context	network-instance name <i>string</i> protocols bgp convergence min-wait-to-advertise <i>number</i>
Tree	min-wait-to-advertise
Description	<p>The minimum amount of time, in seconds, measured from the moment when the first session (configured or dynamic) comes up after a BGP restart, until BGP is allowed to advertise any routes to any peer</p> <p>The sessions that are established when this timer expires determines the set of peers from which EOR is expected in order to declare convergence for an address family. A value of 0 means the feature is disabled and all routes are advertised immediately.</p> <p>This timer and associated state machine are only restarted by one of the following triggers:</p> <ul style="list-style-type: none">• BGP instance admin disable/enable• tools clear network-instance protocols bgp reset-peer• bgp application restart

	<ul style="list-style-type: none">node reboot
Range	0 to 3600
Default	0
Configurable	True

dynamic-neighbors

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors
Tree	dynamic-neighbors
Description	Options related to the acceptance and initiation of dynamic BGP sessions
Configurable	True

accept

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept
Tree	accept
Description	Options related to the acceptance of dynamic BGP sessions from remote peers
Configurable	True

match prefix (*ipv4-prefix | ipv6-prefix*) **group-id-range** *string*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (<i>ipv4-prefix ipv6-prefix</i>) group-id-range <i>string</i>
Tree	match
Description	List of prefix and group-id combinations from which incoming TCP connections to port 179 will be accepted An incoming TCP connection to port 179 is matched to a list entry if: (a)the source IP does not match a configured BGP neighbor address (b)the list entry prefix is the longest prefix match of the source IP (c)the list entry group-id-range includes the LLDP Session Group-ID associated with the source IP.
Configurable	True

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (<i>ipv4-prefix ipv6-prefix</i>) group-id-range <i>string</i>
Description	The IP prefix used to match an incoming dynamic BGP session to a group.
Configurable	True

group-id-range *string*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (ipv4-prefix ipv6-prefix) group-id-range <i>string</i>
Description	A contiguous range of Session Group ID values associated with this match entry or the value 'none'.
Configurable	True

allowed-peer-as *string*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (ipv4-prefix ipv6-prefix) group-id-range <i>string</i> allowed-peer-as <i>string</i>
Tree	allowed-peer-as
Description	The allowed AS numbers that can establish incoming BGP sessions from this prefix and group-id-range combination If the OPEN message from a peer matched to this prefix contains a MyAS number that is not in this allowed list then a NOTIFICATION is sent to the peer with the indication Bad Peer AS. Each entry in this list can be a single AS number or a range of AS numbers in the format as1..as2
Configurable	True
Max. Elements	32

peer-group *reference*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (ipv4-prefix ipv6-prefix) group-id-range <i>string</i> peer-group <i>reference</i>
Tree	peer-group
Description	Reference to a peer-group When an incoming session is matched to this list entry it is associated with the peer-group referenced by this leaf. The peer-group provides all the parameters needed to complete the establishment of the dynamic session. If the referenced peer-group has a configured peer-as this is ignored by dynamic BGP sessions using the group as a template.
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Configurable	True

max-sessions *number*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept max-sessions <i>number</i>
Tree	max-sessions
Description	The maximum number of incoming BGP sessions that will be accepted by the router

A value of 0 means no limit.

Default	0
Configurable	True

initiate

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate
Tree	initiate
Description	Options related to the initiation of dynamic BGP sessions towards remote peers based on LLDP auto-discovery
Configurable	True

match prefix (*ipv4-prefix | ipv6-prefix*) **group-id-range** *string*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate match prefix (<i>ipv4-prefix ipv6-prefix</i>) group-id-range <i>string</i>
Tree	match
Description	List of prefix and group-id combinations learned from LLDP that will trigger BGP to initiate dynamic BGP sessions A dynamic session will be initiated according to a list entry if: (a)the list entry prefix is the longest prefix match of the Peering Address learned from LLDP (b)the list entry group-id-range includes the Session Group-ID learned from LLDP.
Configurable	True

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate match prefix (<i>ipv4-prefix ipv6-prefix</i>) group-id-range <i>string</i>
Description	An IP prefix used to match LLDP Peering Address sub-TLV addresses and which represents a set of valid destinations for outgoing dynamic BGP sessions
Configurable	True

group-id-range *string*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate match prefix (<i>ipv4-prefix ipv6-prefix</i>) group-id-range <i>string</i>
Description	A contiguous range of Session Group ID values associated with this match entry or the value 'none'.
Configurable	True

allowed-peer-as *string*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate match prefix (ipv4-prefix ipv6-prefix) group-id-range <i>string</i> allowed-peer-as <i>string</i>
Tree	allowed-peer-as
Description	The allowed AS numbers associated with outgoing BGP sessions triggered by matching this entry If the router initiates a BGP connection to an LLDP-discovered Peering Address matched to this list entry, and the OPEN message received from the peer contains a MyAS number that is not in this allowed list then a NOTIFICATION is sent to the peer with the indication Bad Peer AS. Each entry in this list can be a single AS number or a range of AS numbers in the format as1..as2
Configurable	True
Max. Elements	32

peer-group *reference*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate match prefix (ipv4-prefix ipv6-prefix) group-id-range <i>string</i> peer-group <i>reference</i>
Tree	peer-group
Description	Reference to a peer-group When an outgoing dynamic session is matched to this list entry it is associated with the peer-group referenced by this leaf. The peer-group provides all the parameters needed to complete the establishment of the dynamic session. If the referenced peer-group has a configured peer-as this is ignored by dynamic BGP sessions using the group as a template.
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Configurable	True

max-sessions *number*

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors initiate max-sessions <i>number</i>
Tree	max-sessions
Description	The maximum number of outgoing dynamic BGP sessions that will be initiated by the router, based on LLDP auto-discovery A value of 0 means no limit.
Default	0
Configurable	True

ebgp-default-policy

Context	network-instance name <i>string</i> protocols bgp ebgp-default-policy
Tree	ebgp-default-policy
Description	Options for controlling the default policies that apply to EBGp sessions
Configurable	True

export-reject-all *boolean*

Context	network-instance name <i>string</i> protocols bgp ebgp-default-policy export-reject-all <i>boolean</i>
Tree	export-reject-all
Description	When set to true, all outbound routes towards any EBGp peer to which no explicit export policy is applied are treated as though they were rejected by policy
Default	true
Configurable	True

import-reject-all *boolean*

Context	network-instance name <i>string</i> protocols bgp ebgp-default-policy import-reject-all <i>boolean</i>
Tree	import-reject-all
Description	When set to true, all inbound routes from any EBGp peer to which no explicit import policy is applied are treated as though they were rejected by policy
Default	true
Configurable	True

export-policy *reference*

Context	network-instance name <i>string</i> protocols bgp export-policy <i>reference</i>
Tree	export-policy
Description	Apply an export policy to advertised BGP routes
Reference	routing-policy policy name <i>string</i>
Configurable	True

failure-detection

Context	network-instance name <i>string</i> protocols bgp failure-detection
Tree	failure-detection
Description	Options related to methods of detecting BGP session failure
Configurable	True

enable-bfd *boolean*

Context	network-instance name <i>string</i> protocols bgp failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Description	The true setting enables Bi-directional Forwarding Detection on BGP sessions belonging to the peer group
Default	false
Configurable	True

fast-failover *boolean*

Context	network-instance name <i>string</i> protocols bgp failure-detection fast-failover <i>boolean</i>
Tree	fast-failover
Description	The true setting causes EBGP and IBGP sessions to drop immediately (and not wait for hold timer expiry) when the local interface that they depend upon for neighbor reachability goes down
Default	true
Configurable	True

graceful-restart

Context	network-instance name <i>string</i> protocols bgp graceful-restart
Tree	graceful-restart
Description	Options for controlling the behavior of the router as a graceful restart helper
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp graceful-restart admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable graceful restart helper for all address families
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

stale-routes-time *number*

Context	network-instance name <i>string</i> protocols bgp graceful-restart stale-routes-time <i>number</i>
Tree	stale-routes-time
Description	The maximum number of seconds that routes received from a helped peer remain stale until they are deleted Routes of AFI/SAFI X received from peer Y are marked stale when peer Y goes down and its previous GR capability included AFI/SAFI X.
Range	1 to 3600
Default	360
Units	seconds
Configurable	True

group **group-name** *string*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Tree	group
Description	Peer group templates
Configurable	True

group-name *string*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Description	The configured name of the peer group
String Length	1 to 255
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the peer group Disable will tear down all the BGP sessions in the group, even if they are administratively enabled at the neighbor level.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

as-path-options

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options
Tree	as-path-options
Description	Options for handling the AS_PATH in received BGP routes
Configurable	True

allow-own-as *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options allow-own-as <i>number</i>
Tree	allow-own-as
Description	The maximum number of times the global AS number or a local AS number of the BGP instance can appear in any received AS_PATH before it is considered a loop and considered invalid When this value is changed the new value applies only to the routes received after the change is committed.
Configurable	True

remove-private-as

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options remove-private-as
Tree	remove-private-as
Description	Container with options for removing private AS numbers (2-byte and 4-byte) from the advertised AS path towards all peers
Configurable	True

ignore-peer-as *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options remove-private-as ignore-peer-as <i>boolean</i>
Tree	ignore-peer-as
Description	If set to true then do not delete or replace a private AS number that is the same as the peer AS number
Default	false
Configurable	True

leading-only *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options remove-private-as leading-only <i>boolean</i>
Tree	leading-only
Description	If set to true then only delete or replace private AS numbers that appear before the first occurrence of a non-private ASN in the sequence of most recent ASNs in the AS path
Default	false
Configurable	True

mode *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options remove-private-as mode <i>keyword</i>
Tree	mode
Description	The method by which private AS numbers are removed from the advertised AS_PATH attribute
Options	<ul style="list-style-type: none">disabled Do not strip or replace any private AS numbersdelete Delete private AS numbers, shortening the AS path

- `replace`
Replace private AS numbers with the local AS number used towards the peer, maintaining the AS path length

Configurable True

replace-peer-as *boolean*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **as-path-options replace-peer-as** *boolean*

Tree **replace-peer-as**

Description If set to true then replace every occurrence of the peer AS number that is present in the advertised AS path with the local AS number used towards the peer

Configurable True

authentication

Context **network-instance name** *string* **protocols bgp group group-name** *string* **authentication**

Tree **authentication**

Description Container with authentication options that apply to all peers in this peer-group

Configurable True

keychain *reference*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **authentication keychain** *reference*

Tree **keychain**

Description Reference to a keychain. The keychain type must be tcp-md5 or tcp-ao.

Reference **system authentication keychain name** *string*

Configurable True

description *string*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **description** *string*

Tree **description**

Description A user provided description string for the peer group

String Length 1 to 255

Configurable True

export-policy *reference*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> export-policy <i>reference</i>
Tree	export-policy
Description	Apply an export policy to advertised BGP routes
Reference	routing-policy policy name <i>string</i>
Configurable	True

failure-detection

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> failure-detection
Tree	failure-detection
Description	Options related to methods of detecting BGP session failure
Configurable	True

enable-bfd *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Description	The true setting enables Bi-directional Forwarding Detection on BGP sessions belonging to the peer group
Configurable	True

fast-failover *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> failure-detection fast-failover <i>boolean</i>
Tree	fast-failover
Description	The true setting causes EBGp and IBGP sessions in the peer group to drop immediately (and not wait for hold timer expiry) when the local interface that they depend upon for neighbor reachability goes down
Configurable	True

graceful-restart

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> graceful-restart
Tree	graceful-restart
Description	Options related to router behavior as a graceful restart helper
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> graceful-restart admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable graceful restart helper for all address families
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

stale-routes-time *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> graceful-restart stale-routes-time <i>number</i>
Tree	stale-routes-time
Description	The maximum number of seconds that routes received from a helped peer remain stale until they are deleted Routes of AFI/SAFI X received from peer Y are marked stale when peer Y goes down and its previous GR capability included AFI/SAFI X.
Range	1 to 3600
Units	seconds
Configurable	True

import-policy *reference*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> import-policy <i>reference</i>
Tree	import-policy
Description	Apply an import policy to received BGP routes
Reference	routing-policy policy name <i>string</i>
Configurable	True

ipv4-unicast

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast
Tree	ipv4-unicast
Description	Options related to the IPv4-unicast address family
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the IPv4 unicast address family on all sessions belonging to the group
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

advertise-ipv6-next-hops *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Description	Enables advertisement of IPv4 routes with IPv6 next-hops to peers in the group When set to true, BGP advertises IPv4-unicast routes to its peers using MP-BGP. If the local-address towards a peer is an IPv6 address and BGP is supposed to apply next-hop-self the MP_REACH_NLRI will encode the IPv6 local-address as the BGP next-hop. When set to false, BGP is required to advertise an IPv4 next-hop with every IPv4 route (and to encode that in the NEXT_HOP attribute).
Configurable	True

prefix-limit

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast prefix-limit
Tree	prefix-limit
Description	Options for configuring the maximum number of IPv4 routes allowed to be received from each peer in the group
Configurable	True

max-received-routes *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes
Description	Maximum number of IPv4 routes that will be accepted from each neighbor, counting routes accepted and rejected by import policies
Range	1 to 4294967295
Default	4294967295
Configurable	True

warning-threshold-pct *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Description	When the number of IPv4 routes received from any group peer (counting routes accepted and rejected by import policy) reaches this percentage of the max-received-routes limit, BGP raises a warning log event
Range	0 to 100
Default	90
Configurable	True

receive-ipv6-next-hops *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast receive-ipv6-next-hops <i>boolean</i>
Tree	receive-ipv6-next-hops
Description	Enables the advertisement of the RFC 5549 capability to receive IPv4 routes with IPv6 next-hops When set to true, BGP advertises an extended NH encoding (RFC 5549) capability to its peers. This capability indicates that local router is prepared to accept BGP routes for IPv4 NLRI with IPv6 next-hops from peers in the scope of the command. When set to false, BGP handles received IPV4 routes with IPv6 next-hops as an error and applies treat-as-withdraw.
Configurable	True

ipv6-unicast

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast
Tree	ipv6-unicast
Description	Options related to the IPv6-unicast address family
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the IPv6 unicast address family on all sessions belonging to the group
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

prefix-limit

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast prefix-limit
Tree	prefix-limit
Description	Options for configuring the maximum number of IPv6 routes allowed to be received from each peer in the group
Configurable	True

max-received-routes *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes
Description	Maximum number of IPv6 routes that will be accepted from each neighbor, counting routes accepted and rejected by import policies
Range	1 to 4294967295
Default	4294967295
Configurable	True

warning-threshold-pct *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Description	When the number of IPv6 routes received from any group peer (counting routes accepted and rejected by import policy) reaches this percentage of the max-received-routes limit, BGP raises a warning log event
Range	0 to 100
Default	90
Configurable	True

local-as as-number *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> local-as as-number <i>number</i>
Tree	local-as
Description	Options related to the local autonomous-system number advertised by this router to its peers
Configurable	True
Max. Elements	1

as-number *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> local-as as-number <i>number</i>
Description	The local autonomous system number used to override the global ASN on this group of BGP sessions Sets the ASN value that this router sends in its OPEN message towards its peer in the group.
Range	1 to 4294967295
Configurable	True

prepend-global-as *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> local-as as-number <i>number</i> prepend-global-as <i>boolean</i>
Tree	prepend-global-as
Description	When set to true, the global ASN value is prepended to the AS path in outbound routes towards each BGP peer in the group

If a session is EBGp (peer-as is not equal to the local-as) then the local-as is prepended as the final step, so that the local-as is the first element in the AS_PATH received by the peer.

Default true
Configurable True

prepend-local-as *boolean*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **local-as as-number** *number* **prepend-local-as** *boolean*

Tree **prepend-local-as**

Description When set to true, the local AS value is prepended to the AS path of inbound routes from each EBGp peer belonging to the group

Default true
Configurable True

local-preference *number*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **local-preference** *number*

Tree **local-preference**

Description The value of the local-preference attribute that is added to received routes from EBGp peers in the group

It is also used to encode the local preference attribute for locally generated BGP routes.

Configurable True

maintenance-group *string*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **maintenance-group** *string*

Tree **maintenance-group**

Description State field to display the maintenance group to which this group belongs to.

Configurable False

next-hop-self *boolean*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **next-hop-self** *boolean*

Tree **next-hop-self**

Description Enables next-hop-self in outbound routes towards each peer in the group

When set to true, the next-hop in all BGP routes advertised to each group peer is set equal to the local-address used on the sessions (or to the router ID if the NLRI is IPv6 and there is no IPv6 local address to use). This is independent of the route origin (EBGP, IBGP or redistributed direct/static/aggregate route). When set to false, normal BGP rules from RFC 4271 apply.

Default false
Configurable True

peer-as number

Context **network-instance name** *string* **protocols bgp group group-name** *string* **peer-as** *number*
Tree **peer-as**
Description The autonomous system number expected from each peer in the group
A configured session with a peer does not come up if this value does not match the AS value reported by the peer in its OPEN message.
Range 1 to 4294967295
Configurable True

route-reflector

Context **network-instance name** *string* **protocols bgp group group-name** *string* **route-reflector**
Tree **route-reflector**
Description Container with route reflection configuration options.
Configurable True

client boolean

Context **network-instance name** *string* **protocols bgp group group-name** *string* **route-reflector** **client** *boolean*
Tree **client**
Description When this is set to true all configured and dynamic BGP sessions that belong to the peer-group are considered RR clients.
Configurable True

cluster-id *string*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> route-reflector cluster-id <i>string</i>
Tree	cluster-id
Description	The cluster-id to insert into the CLUSTER_LIST attribute when reflecting routes received by or sent to each client in the peer-group. The default is inherited from instance level configuration.
Configurable	True

send-community

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-community
Tree	send-community
Description	Options for controlling the sending of BGP communities to peers in the group
Configurable	True

large *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-community large <i>boolean</i>
Tree	large
Description	The false setting causes BGP to strip all large (12 byte) BGP communities from all outbound routes advertised to each peer in the group
Configurable	True

standard *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-community standard <i>boolean</i>
Tree	standard
Description	The false setting causes BGP to strip all standard (4 byte) communities from all outbound routes advertised to each peer in the group
Configurable	True

send-default-route

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-default-route
Tree	send-default-route
Description	Options for controlling the generation of default routes towards group peers
Configurable	True

export-policy *reference*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-default-route export-policy <i>reference</i>
Tree	export-policy
Description	The name of a policy that should be applied to the advertised default routes, in order to set their attributes to non-default values Only the default-action of this policy is parsed and applied.
Reference	routing-policy policy name <i>string</i>
Configurable	True

ipv4-unicast *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-default-route ipv4-unicast <i>boolean</i>
Tree	ipv4-unicast
Description	Enables the sending of a synthetically generated default IPv4 route [0/0] to each peer in the group
Default	false
Configurable	True

ipv6-unicast *boolean*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-default-route ipv6-unicast <i>boolean</i>
Tree	ipv6-unicast
Description	Enables the sending of a synthetically generated default IPv6 route [::/0] to each peer in the group
Default	false
Configurable	True

statistics

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics
Tree	statistics
Description	Container for BGP statistics.
Configurable	False

disabled-peers *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics disabled-peers <i>number</i>
Tree	disabled-peers
Description	The number of configured BGP peers associated with the peer-group that are administratively disabled
Configurable	False

dynamic-peers *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics dynamic-peers <i>number</i>
Tree	dynamic-peers
Description	The number of dynamic BGP peers associated with the peer-group that are currently in the established state, counting sessions resulting from accepted incoming TCP connections and outgoing TCP connections triggered by LLDP auto-discovery
Configurable	False

path-memory *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics path-memory <i>number</i>
Tree	path-memory
Description	The total number of bytes required to store the path attribute objects used by received BGP routes associated with the peer-group
Default	0
Configurable	False

total-active-routes *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics total-active-routes <i>number</i>
Tree	total-active-routes
Description	The total number of received BGP routes that are active (installed for forwarding) and associated with the peer-group, summed across all address families
Default	0
Configurable	False

total-paths *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics total-paths <i>number</i>
Tree	total-paths
Description	The total number of path attribute objects used by received BGP routes associated with the peer-group
Default	0
Configurable	False

total-peers *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics total-peers <i>number</i>
Tree	total-peers
Description	The total number of configured BGP peers associated with the peer-group
Configurable	False

total-prefixes *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics total-prefixes <i>number</i>
Tree	total-prefixes
Description	The total number of unique NLRI contained in all received BGP routes associated with the BGP instance or the peer-group.
Configurable	False

total-received-routes *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics total-received-routes <i>number</i>
Tree	total-received-routes
Description	The total number of received BGP routes associated with the peer-group, summed across all address families
Default	0
Configurable	False

up-peers *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics up-peers <i>number</i>
Tree	up-peers
Description	The number of configured BGP peers associated with the peer-group that are currently in the established state
Configurable	False

timers

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers
Tree	timers
Description	Enter timer context
Configurable	True

connect-retry *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers connect-retry <i>number</i>
Tree	connect-retry
Description	The time interval in seconds between successive attempts to establish a session with a peer
Range	1 to 65535
Default	120
Units	seconds
Configurable	True

hold-time *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers hold-time <i>number</i>
Tree	hold-time
Description	The hold-time interval in seconds that the router proposes to the peer in its OPEN message The actual in-use hold-time is negotiated to the lowest value proposed by the two peers. A negotiated value of 0 suppresses the sending of keepalives by both peers.
Range	0 3 to 65535
Default	90
Units	seconds
Configurable	True

keepalive-interval *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers keepalive-interval <i>number</i>
Tree	keepalive-interval
Description	The interval in seconds between successive keepalive messages sent to the peer The period between one keepalive message and the next is the minimum of this configured value and 1/3 of the negotiated hold-time duration. A value of 0 suppresses the sending of keepalives to the peer.
Range	0 to 21845
Units	seconds
Configurable	True

minimum-advertisement-interval *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers minimum-advertisement-interval <i>number</i>
Tree	minimum-advertisement-interval
Description	The value assigned to the MinRouteAdvertisementIntervalTimer of RFC 4271, for both EBGp and IBGP sessions

Each session runs its own independent timer and the timer affects both route advertisements and route withdrawals, regardless of address family. For route withdrawals only, this timer is bypassed if rapid-withdrawal is set to true.

Range	1 to 255
Default	5
Units	seconds
Configurable	True

trace-options

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options
Tree	trace-options
Description	Debug traceoptions for BGP
Configurable	True

flag name keyword

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options flag name <i>keyword</i>
Tree	flag
Description	Tracing parameters
Configurable	True

name keyword

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options flag name <i>keyword</i>
Description	
Options	<ul style="list-style-type: none">• events Trace all BGP events.• packets Trace all BGP protocol packets.• open Trace BGP open packets.• keepalive Trace BGP keepalive packets.• graceful-restart Trace Graceful Restart events.• timers

	Trace routing protocol timer processing.
	<ul style="list-style-type: none">• route
	Trace BGP route table manager.
	<ul style="list-style-type: none">• notification
	Trace Bgp notification.
	<ul style="list-style-type: none">• socket
	Trace socket info.
	<ul style="list-style-type: none">• update
	Trace update info.
Configurable	True

modifier *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options flag name <i>keyword</i> modifier <i>keyword</i>
Tree	modifier
Description	
Options	<ul style="list-style-type: none">• detail To enable detailed tracing. Includes both received and sent packets.• receive To enable tracing for the packets which are received.• send To enable tracing for the sent packets.
Configurable	True

transport

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> transport
Tree	transport
Description	
Configurable	True

local-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> transport local-address (<i>ipv4-address ipv6-address</i>)
Tree	local-address
Description	The local TCP endpoint of used for all BGP sessions in the group

This also the source address for next-hop-self, if it applies. The local-address can be specified as an IP address that is resolvable to a local interface or else it can refer to a subinterface directly, by name

Configurable True

passive-mode *boolean*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **transport passive-mode** *boolean*

Tree **passive-mode**

Description The true setting causes BGP to wait for the peer to initiate the TCP connection
The false setting causes BGP to initiate a TCP connection whenever the BGP session is started or restarted.

Default false

Configurable True

tcp-mss *number*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **transport tcp-mss** *number*

Tree **tcp-mss**

Description The maximum segment size for each BGP TCP session belonging to the group
If the configured tcp-mss value is higher than the discovered path MTU it has no effect and the path MTU is used as the operational TCP MSS.

Range 536 to 9446

Units bytes

Configurable True

under-maintenance *boolean*

Context **network-instance name** *string* **protocols bgp group group-name** *string* **under-maintenance** *boolean*

Tree **under-maintenance**

Description State field to determine if this bgp group is in maintenance mode.

Configurable False

import-policy *reference*

Context	network-instance name <i>string</i> protocols bgp import-policy <i>reference</i>
Tree	import-policy
Description	Apply an import policy to received BGP routes
Reference	routing-policy policy name <i>string</i>
Configurable	True

ipv4-unicast

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast
Tree	ipv4-unicast
Description	Options related to the IPv4-unicast address family
Configurable	True

active-routes *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast active-routes <i>number</i>
Tree	active-routes
Description	The total number of received IPv4 unicast routes that are currently used for forwarding
Default	0
Configurable	False

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the IPv4 unicast address family on all sessions
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

advertise-ipv6-next-hops *boolean*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Description	Enables advertisement of IPv4 routes with IPv6 next-hops to peers When set to true, BGP advertises IPv4-unicast routes to its peers using MP-BGP. If the local-address towards a peer is an IPv6 address and BGP is supposed to apply next-hop-self the MP_REACH_NLRI will encode the IPv6 local-address as the BGP next-hop. When set to false, BGP is required to advertise an IPv4 next-hop with every IPv4 route (and to encode that in the NEXT_HOP attribute).
Default	false
Configurable	True

convergence

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence
Tree	convergence
Description	Options for controlling and monitoring routing convergence of the relevant address family
Configurable	True

converged-peers *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence converged-peers <i>number</i>
Tree	converged-peers
Description	The number of peers that have sent an EOR marker for the address family since the last BGP restart
Configurable	False

convergence-state *keyword*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence convergence-state <i>keyword</i>
Tree	convergence-state
Description	
Options	<ul style="list-style-type: none">• waiting BGP has recently restarted and no sessions have re-established yet• started

- BGP has recently restarted and at least one session has re-established with support of the address family
- partial
BGP has recently restarted and at least one session has advertised an End-of-RIB marker for the address family.
- timeout
BGP has recently restarted and not all non-slow peers advertised an End-of-RIB marker for the address family before the max-wait-to-advertise timer expired
- converged
All non-slow peers that support the address family have have advertised the End-of-RIB marker for the address family

Configurable False

convergence-time *number*

Context **network-instance name** *string* **protocols bgp ipv4-unicast convergence convergence-time** *number*

Tree **convergence-time**

Description The elapsed time in seconds, starting from the last BGP restart, to reach the converged state for the address family

Configurable False

first-up-peer-time *number*

Context **network-instance name** *string* **protocols bgp ipv4-unicast convergence first-up-peer-time** *number*

Tree **first-up-peer-time**

Description The time when the first session supporting the address family came up, measured from the time that the BGP instance restarted

Configurable False

last-up-peer-time *number*

Context **network-instance name** *string* **protocols bgp ipv4-unicast convergence last-up-peer-time** *number*

Tree **last-up-peer-time**

Description The time when the last session supporting the address family came up, measured from the time that the BGP instance restarted

Configurable False

max-wait-to-advertise *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence max-wait-to-advertise <i>number</i>
Tree	max-wait-to-advertise
Description	<p>The maximum amount of time, in seconds, measured from the time when the first session (configured or dynamic) that supports the address family comes up after a BGP restart, until BGP is allowed to advertise any routes in that address family to any peer</p> <p>The value of this leaf must always be greater than or equal to the operational value of min-wait-to-advertise. The default value is 3x the value of min-wait-to-advertise. A value of 0 means the feature is disabled and there is no additional delay before advertising routes of the address family.</p>
Range	0 to 3600
Default	0
Configurable	True

oper-max-wait-to-advertise *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence oper-max-wait-to-advertise <i>number</i>
Tree	oper-max-wait-to-advertise
Description	The operational value of the max-wait-to-advertise timer for the address family
Range	0 to 10800
Configurable	False

up-peers *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence up-peers <i>number</i>
Tree	up-peers
Description	The number of BGP sessions (configured and dynamic) that support the address family and that are currently in the established state
Configurable	False

up-peers-when-min-expired *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence up-peers-when-min-expired <i>number</i>
Tree	up-peers-when-min-expired
Description	The number of BGP sessions (configured and dynamic) that support the address family and that were in established state when the win-wait-to-advertise timer expired
Configurable	False

multipath

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath
Tree	multipath
Description	Options related to BGP multipath
Configurable	True

allow-multiple-as *boolean*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath allow-multiple-as <i>boolean</i>
Tree	allow-multiple-as
Description	When set to true, BGP is allowed to build a multipath set using BGP routes with different neighbor AS (most recent AS in the AS_PATH) When set to false, BGP is only allowed to use non-best paths for ECMP if they meet the multipath criteria and they have the same neighbor AS as the best path
Default	true
Configurable	True

max-paths-level-1 *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath max-paths-level-1 <i>number</i>
Tree	max-paths-level-1
Description	The maximum number of BGP ECMP next-hops for BGP routes with an NLRI belonging to the address family of this configuration context
Range	1 to 128
Default	1
Configurable	True

max-paths-level-2 *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath max-paths-level-2 <i>number</i>
Tree	max-paths-level-2
Description	The maximum number of resolving ECMP next-hops per BGP next-hop associated with BGP routes having an NLRI belonging to the address family of this configuration context
Range	1 to 128
Default	1
Configurable	True

receive-ipv6-next-hops *boolean*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast receive-ipv6-next-hops <i>boolean</i>
Tree	receive-ipv6-next-hops
Description	Enables the advertisement of the RFC 5549 capability to receive IPv4 routes with IPv6 next-hops When set to true, BGP advertises an extended NH encoding (RFC 5549) capability to its peers. This capability indicates that local router is prepared to accept BGP routes for IPv4 NLRI with IPv6 next-hops from peers in the scope of the command. When set to false, BGP handles received IPV4 routes with IPv6 next-hops as an error and applies treat-as-withdraw.
Default	false
Configurable	True

received-routes *number*

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast received-routes <i>number</i>
Tree	received-routes
Description	The total number of IPv4 unicast routes received from all peers of the BGP instance
Default	0
Configurable	False

ipv6-unicast

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast
Tree	ipv6-unicast
Description	Options related to the IPv6-unicast address family
Configurable	True

active-routes *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast active-routes <i>number</i>
Tree	active-routes
Description	The total number of received IPv6 unicast routes that are currently used for forwarding
Default	0
Configurable	False

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the IPv6 unicast address family on all sessions
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

convergence

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence
Tree	convergence
Description	Options for controlling and monitoring routing convergence of the relevant address family
Configurable	True

converged-peers *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence converged-peers <i>number</i>
Tree	converged-peers
Description	The number of peers that have sent an EOR marker for the address family since the last BGP restart
Configurable	False

convergence-state *keyword*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence convergence-state <i>keyword</i>
Tree	convergence-state
Description	
Options	<ul style="list-style-type: none">• waiting BGP has recently restarted and no sessions have re-established yet• started BGP has recently restarted and at least one session has re-established with support of the address family• partial BGP has recently restarted and at least one session has advertised an End-of-RIB marker for the address family.• timeout BGP has recently restarted and not all non-slow peers advertised an End-of-RIB marker for the address family before the max-wait-to-advertise timer expired• converged All non-slow peers that support the address family have have advertised the End-of-RIB marker for the address family
Configurable	False

convergence-time *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence convergence-time <i>number</i>
Tree	convergence-time
Description	The elapsed time in seconds, starting from the last BGP restart, to reach the converged state for the address family
Configurable	False

first-up-peer-time *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence first-up-peer-time <i>number</i>
Tree	first-up-peer-time
Description	The time when the first session supporting the address family came up, measured from the time that the BGP instance restarted
Configurable	False

last-up-peer-time *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence last-up-peer-time <i>number</i>
Tree	last-up-peer-time
Description	The time when the last session supporting the address family came up, measured from the time that the BGP instance restarted
Configurable	False

max-wait-to-advertise *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence max-wait-to-advertise <i>number</i>
Tree	max-wait-to-advertise
Description	<p>The maximum amount of time, in seconds, measured from the time when the first session (configured or dynamic) that supports the address family comes up after a BGP restart, until BGP is allowed to advertise any routes in that address family to any peer</p> <p>The value of this leaf must always be greater than or equal to the operational value of min-wait-to-advertise. The default value is 3x the value of min-wait-to-advertise. A value of 0 means the feature is disabled and there is no additional delay before advertising routes of the address family.</p>
Range	0 to 3600
Default	0
Configurable	True

oper-max-wait-to-advertise *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence oper-max-wait-to-advertise <i>number</i>
Tree	oper-max-wait-to-advertise
Description	The operational value of the max-wait-to-advertise timer for the address family
Range	0 to 10800
Configurable	False

up-peers *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence up-peers <i>number</i>
Tree	up-peers
Description	The number of BGP sessions (configured and dynamic) that support the address family and that are currently in the established state
Configurable	False

up-peers-when-min-expired *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence up-peers-when-min-expired <i>number</i>
Tree	up-peers-when-min-expired
Description	The number of BGP sessions (configured and dynamic) that support the address family and that were in established state when the win-wait-to-advertise timer expired
Configurable	False

multipath

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath
Tree	multipath
Description	Options related to BGP multipath
Configurable	True

allow-multiple-as *boolean*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath allow-multiple-as <i>boolean</i>
Tree	allow-multiple-as
Description	When set to true, BGP is allowed to build a multipath set using BGP routes with different neighbor AS (most recent AS in the AS_PATH) When set to false, BGP is only allowed to use non-best paths for ECMP if they meet the multipath criteria and they have the same neighbor AS as the best path
Default	true
Configurable	True

max-paths-level-1 *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath max-paths-level-1 <i>number</i>
Tree	max-paths-level-1
Description	The maximum number of BGP ECMP next-hops for BGP routes with an NLRI belonging to the address family of this configuration context
Range	1 to 128
Default	1
Configurable	True

max-paths-level-2 *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath max-paths-level-2 <i>number</i>
Tree	max-paths-level-2
Description	The maximum number of resolving ECMP next-hops per BGP next-hop associated with BGP routes having an NLRI belonging to the address family of this configuration context
Range	1 to 128
Default	1
Configurable	True

received-routes *number*

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast received-routes <i>number</i>
Tree	received-routes
Description	The total number of IPv6 unicast routes received from all peers of the BGP instance
Default	0
Configurable	False

local-preference *number*

Context	network-instance name <i>string</i> protocols bgp local-preference <i>number</i>
Tree	local-preference
Description	The value of the local-preference attribute that is added to received routes from EBGP peers It is also used to encode the local preference attribute for locally generated BGP routes.
Default	100
Configurable	True

maintenance-group *string*

Context	network-instance name <i>string protocols bgp maintenance-group</i> <i>string</i>
Tree	maintenance-group
Description	State field to display the maintenance group to which this bgp instance belongs to.
Configurable	False

neighbor peer-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string protocols bgp neighbor peer-address</i> (<i>ipv4-address ipv6-address</i>)
Tree	neighbor
Description	Create a configured BGP session
Configurable	True

peer-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string protocols bgp neighbor peer-address</i> (<i>ipv4-address ipv6-address</i>)
Description	The transport address of the BGP peer The peer-address must be a valid IPv4 unicast address or a valid IPv6 global unicast address. Sessions to a link-local IPv6 address are not supported.
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string protocols bgp neighbor peer-address</i> (<i>ipv4-address ipv6-address</i>) admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the peer Disable will tear down the BGP session (return it to IDLE state).
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

advertised-capabilities *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) advertised-capabilities <i>keyword</i>
Tree	advertised-capabilities
Description	List of BGP capabilities advertised by the local routing device to the peer
Options	<ul style="list-style-type: none">• MP_BGP• ROUTE_REFRESH• EXT_NH_ENCODING• GRACEFUL_RESTART• 4-OCTET_ASN• ORF_SEND_EXCOMM• ORF_RECEIVE_EXCOMM
Configurable	False

as-path-options

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) as-path-options
Tree	as-path-options
Description	Options for handling the AS_PATH in received BGP routes
Configurable	True

allow-own-as *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) as-path-options allow-own-as <i>number</i>
Tree	allow-own-as
Description	The maximum number of times the global AS number or a local AS number of the BGP instance can appear in any received AS_PATH before it is considered a loop and considered invalid
Configurable	True

remove-private-as

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) as-path-options remove-private-as
Tree	remove-private-as
Description	Container with options for removing private AS numbers (2-byte and 4-byte) from the advertised AS path towards all peers
Configurable	True

ignore-peer-as *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) as-path-options remove-private-as ignore-peer-as <i>boolean</i>
Tree	ignore-peer-as
Description	If set to true then do not delete or replace a private AS number that is the same as the peer AS number
Default	false
Configurable	True

leading-only *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) as-path-options remove-private-as leading-only <i>boolean</i>
Tree	leading-only
Description	If set to true then only delete or replace private AS numbers that appear before the first occurrence of a non-private ASN in the sequence of most recent ASNs in the AS path
Default	false
Configurable	True

mode *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) as-path-options remove-private-as mode <i>keyword</i>
Tree	mode
Description	The method by which private AS numbers are removed from the advertised AS_PATH attribute
Options	<ul style="list-style-type: none">disabled Do not strip or replace any private AS numbersdelete Delete private AS numbers, shortening the AS path

- `replace`
Replace private AS numbers with the local AS number used towards the peer, maintaining the AS path length

Configurable True

replace-peer-as *boolean*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **as-path-options replace-peer-as** *boolean*

Tree **replace-peer-as**

Description If set to true then replace every occurrence of the peer AS number that is present in the advertised AS path with the local AS number used towards the peer

Configurable True

authentication

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **authentication**

Tree **authentication**

Description Container with authentication options that apply to this specific peer

Configurable True

keychain *reference*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **authentication keychain** *reference*

Tree **keychain**

Description Reference to a keychain. The keychain type must be tcp-md5 or tcp-ao.

Reference **system authentication keychain name** *string*

Configurable True

description *string*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **description** *string*

Tree **description**

Description A user provided description string for the peer

String Length 1 to 255

Configurable True

discovered-by-lldp *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) discovered-by-lldp <i>boolean</i>
Tree	discovered-by-lldp
Description	Set to true if the peer IP address is known through LLDP (irrespective of whether the final TCP connection was originated by this router or not)
Configurable	False

dynamic-neighbor *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) dynamic-neighbor <i>boolean</i>
Tree	dynamic-neighbor
Description	Indicates true if the neighbor is a dynamic peer that resulted from an accepted incoming TCP connection or an outgoing TCP connection triggered by LLDP auto-discovery
Configurable	False

established-transitions *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) established-transitions <i>number</i>
Tree	established-transitions
Description	The total number of times the BGP FSM transitioned into the established state for this peer
Default	0
Configurable	False

export-policy *reference*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) export-policy <i>reference</i>
Tree	export-policy
Description	Apply an export policy to advertised BGP routes
Reference	routing-policy policy name <i>string</i>
Configurable	True

failure-detection

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) failure-detection
Tree	failure-detection
Description	Options related to methods of detecting BGP session failure
Configurable	True

enable-bfd *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Description	The true setting enables Bi-directional Forwarding Detection on BGP sessions belonging to the peer group
Configurable	True

fast-failover *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) failure-detection fast-failover <i>boolean</i>
Tree	fast-failover
Description	The true setting the EBGP or IBGP session to drop immediately (and not wait for hold timer expiry) when the local interface that it depends upon for neighbor reachability goes down
Configurable	True

graceful-restart

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart
Tree	graceful-restart
Description	Options related to router behavior as a graceful restart helper
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable graceful restart helper for all address families
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

helper-active *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart helper-active <i>boolean</i>
Tree	helper-active
Description	Set to true when the router is actively helping the neighbor for at least one address family – i.e. for that address family the peer restarted with F=1 in its capability and the stale-routes-time has not expired yet
Configurable	False

last-restart-time *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart last-restart-time <i>string</i>
Tree	last-restart-time
Description	The last time the peer restarted
Configurable	False

neighbor-capability

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart neighbor-capability
Tree	neighbor-capability
Description	Container for information about the last GR capability received from the neighbor
Configurable	False

afi-safi *name keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart neighbor-capability afi-safi name <i>keyword</i>
Tree	afi-safi
Description	List of AFI/SAFI TLVs that were contained in the neighbor's last GR capability
Configurable	False

name *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart neighbor-capability afi-safi name <i>keyword</i>
Description	
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	False

forwarding-preserved *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart neighbor-capability afi-safi name <i>keyword</i> forwarding-preserved <i>boolean</i>
Tree	forwarding-preserved
Description	The F-bit setting in the AFI/SAFI TLV
Configurable	False

restart-time *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart neighbor-capability restart-time <i>number</i>
Tree	restart-time
Description	The value of the Restart Time in the neighbor's last GR capability
Configurable	False

number-of-restarts *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart number-of-restarts <i>number</i>
Tree	number-of-restarts
Description	The number of times the peer has restarted
Configurable	False

stale-routes-time *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) graceful-restart stale-routes-time <i>number</i>
Tree	stale-routes-time
Description	The maximum number of seconds that routes received from a helped peer remain stale until they are deleted Routes of AFI/SAFI X received from peer Y are marked stale when peer Y goes down and its previous GR capability included AFI/SAFI X.
Range	1 to 3600
Units	seconds
Configurable	True

import-policy *reference*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) import-policy <i>reference</i>
Tree	import-policy
Description	Apply an import policy to received BGP routes
Reference	routing-policy policy name <i>string</i>
Configurable	True

ipv4-unicast

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv4-unicast
Tree	ipv4-unicast
Description	Options related to the IPv4-unicast address family
Configurable	True

active-routes *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv4-unicast active-routes <i>number</i>
Tree	active-routes
Description	The number of IPv4 unicast received from the peer that are currently used for forwarding
Configurable	False

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv4-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the IPv4 unicast address family on the BGP session
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

advertise-ipv6-next-hops *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv4-unicast advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Description	Enables advertisement of IPv4 routes with IPv6 next-hops to the peer When set to true, BGP advertises IPv4-unicast routes using MP-BGP. If the local-address towards the peer is an IPv6 address and BGP is supposed to apply next-hop-self the MP_REACH_NLRI will encode the IPv6 local-address as the BGP next-hop. When set to false, BGP is required to advertise an IPv4 next-hop with every IPv4 route (and to encode that in the NEXT_HOP attribute).
Configurable	True

oper-state *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv4-unicast oper-state <i>keyword</i>
Tree	oper-state
Description	
Options	<ul style="list-style-type: none">• up Negotiated operational state of the IPv4 unicast address family is up• down

Negotiated operational state of the IPv4 unicast address family is down

Configurable False

prefix-limit

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast prefix-limit**

Tree **prefix-limit**

Description Options for configuring the maximum number of IPv4 routes allowed to be received from the peer

Configurable True

max-received-routes *number*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast prefix-limit max-received-routes** *number*

Tree **max-received-routes**

Description Maximum number of IPv4 routes that will be accepted from the neighbor, counting routes accepted and rejected by import policies

Range 1 to 4294967295

Configurable True

warning-threshold-pct *number*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast prefix-limit warning-threshold-pct** *number*

Tree **warning-threshold-pct**

Description When the number of IPv4 routes received from the peer (counting routes accepted and rejected by import policy) reaches this percentage of the max-received-routes limit, BGP raises a warning log event

Range 0 to 100

Configurable True

receive-ipv6-next-hops *boolean*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast receive-ipv6-next-hops** *boolean*

Tree **receive-ipv6-next-hops**

Description Enables the advertisement of the RFC 5549 capability to receive IPv4 routes with IPv6 next-hops

When set to true, BGP advertises an extended NH encoding (RFC 5549) capability to the peer. This capability indicates that local router is prepared to accept BGP routes for IPv4 NLRI with IPv6 next-hops from the peer. When set to false, BGP handles received IPV4 routes with IPv6 next-hops as an error and applies treat-as-withdraw.

Configurable True

received-routes *number*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast received-routes** *number*

Tree **received-routes**

Description The number of IPv4 unicast routes received from the peer, including routes rejected by import policy

Configurable False

rejected-routes *number*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast rejected-routes** *number*

Tree **rejected-routes**

Description The number of IPv4 unicast routes received from the peer that were rejected by import policy

Configurable False

sent-routes *number*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv4-unicast sent-routes** *number*

Tree **sent-routes**

Description The number of IPv4 unicast routes advertised as reachable to the peer

Configurable False

ipv6-unicast

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **ipv6-unicast**

Tree **ipv6-unicast**

Description Options related to the IPv6-unicast address family

Configurable True

active-routes *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast active-routes <i>number</i>
Tree	active-routes
Description	The number of IPv6 unicast received from the peer that are currently used for forwarding
Configurable	False

admin-state *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the IPv6 unicast address family on the BGP session
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast oper-state <i>keyword</i>
Tree	oper-state
Description	
Options	<ul style="list-style-type: none">• up Negotiated operational state of the IPv6 unicast address family is up• down Negotiated operational state of the IPv6 unicast address family is down
Configurable	False

prefix-limit

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast prefix-limit
Tree	prefix-limit
Description	Options for configuring the maximum number of IPv6 routes allowed to be received from the peer
Configurable	True

max-received-routes *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes
Description	Maximum number of IPv6 routes that will be accepted from the neighbor, counting routes accepted and rejected by import policies
Range	1 to 4294967295
Configurable	True

warning-threshold-pct *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Description	When the number of IPv6 routes received from the peer (counting routes accepted and rejected by import policy) reaches this percentage of the max-received-routes limit, BGP raises a warning log event
Range	0 to 100
Configurable	True

received-routes *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast received-routes <i>number</i>
Tree	received-routes
Description	The number of IPv6 unicast routes received from the peer, including routes rejected by import policy
Configurable	False

rejected-routes *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast rejected-routes <i>number</i>
Tree	rejected-routes
Description	The number of IPv6 unicast routes received from the peer that were rejected by import policy
Configurable	False

sent-routes *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) ipv6-unicast sent-routes <i>number</i>
Tree	sent-routes
Description	The number of IPv6 unicast routes advertised as reachable to the peer
Configurable	False

last-established *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) last-established <i>string</i>
Tree	last-established
Description	The time when the session last transitioned into or out of the established state Uptime or downtime of the session can be calculated from this state.
Configurable	False

last-event *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) last-event <i>keyword</i>
Tree	last-event
Description	
Options	<ul style="list-style-type: none">• none• start• stop• open• close• openFail• error• connectRetry• holdTime• keepAlive• recvOpen• recvKeepAlive• recvUpdate• recvNotify• startPassive• parseError

- outOfMemory
- rtmLimitExceed
- outOfProtNHIndex
- outOfNHIndex
- labelAllocFailed
- lspIdAllocFailed
- collisionResolution
- adminShutdown
- adminReset
- configChange
- maxPrefixExceed
- maxPfxExcdLog
- trackingPolMismatch
- receivedMalformedAttr
- adminResetHard
- peerDamping

Configurable False

last-notification-error-code *keyword*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **last-notification-error-code** *keyword*

Tree **last-notification-error-code**

Description The error code in the last NOTIFICATION sent to this peer.

- Options
- Message Header Error
 - Open Message Error
 - Update Message Error
 - Hold Timer Error
 - Finite State Machine Error
 - Cease

Configurable False

last-notification-error-subcode *keyword*

Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **last-notification-error-subcode** *keyword*

Tree **last-notification-error-subcode**

Description The error subcode in the last NOTIFICATION sent to this peer.

- Options
- Connection Not Synchronized

- Bad Message Length
- Bad Message Type
- Unsupported Version Number
- Bad Peer As
- Bad BGP Identifier
- Unsupported Optional Parameter
- Unacceptable Hold Time
- UPDATE Message Error subcodes
- Malformed Attribute List
- Unrecognized Well-known Attribute
- Missing Well-known Attribute
- Attribute Flags Error
- Attribute Length Error
- Invalid ORIGIN Attribute
- Invalid NEXT_HOP Attribute
- Optional Attribute Error
- Invalid Network Field
- Malformed AS_PATH
- Maximum Number of Prefixes Reached
- Administrative Shutdown
- Peer De-configured
- Administrative Reset
- Connection Rejected
- Other Configuration Change
- Connection Collision Resolution
- Out of Resources

Configurable False

last-state *keyword*

Context **network-instance name** *string protocols bgp neighbor peer-address (ipv4-address | ipv6-address)* **last-state** *keyword*

Tree **last-state**

Description Previous state of the session

- Options
- idle
 - connect
 - active
 - opensent
 - openconfirm

	<ul style="list-style-type: none">established
Configurable	False

local-as as-number *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) local-as as-number <i>number</i>
Tree	local-as
Description	Options related to the local autonomous-system number advertised by this router to the peer
Configurable	True
Max. Elements	1

as-number *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) local-as as-number <i>number</i>
Description	The local autonomous system number used to override the global ASN on this session Sets the ASN value that this router sends in its OPEN message towards its peer.
Range	1 to 4294967295
Configurable	True

prepend-global-as *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) local-as as-number <i>number</i> prepend-global-as <i>boolean</i>
Tree	prepend-global-as
Description	When set to true, the global ASN value is prepended to the AS path in outbound routes towards the peer If a session is EBGP (peer-as is not equal to the local-as) then the local-as is prepended as the final step, so that the local-as is the first element in the AS_PATH received by the peer.
Configurable	True

prepend-local-as *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) local-as as-number <i>number</i> prepend-local-as <i>boolean</i>
Tree	prepend-local-as
Description	When set to true, the local AS value is prepended to the AS path of inbound routes from the peer
Configurable	True

local-preference *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) local-preference <i>number</i>
Tree	local-preference
Description	The value of the local-preference attribute that is added to received routes from the peer, if it is EBGP It is also used to encode the local preference attribute for locally generated BGP routes.
Configurable	True

maintenance-group *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) maintenance-group <i>string</i>
Tree	maintenance-group
Description	State field to display the maintenance group to which this neighbor belongs to.
Configurable	False

next-hop-self *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) next-hop-self <i>boolean</i>
Tree	next-hop-self
Description	Enables next-hop-self in outbound routes towards the peer When set to true, the next-hop in all BGP routes advertised to the peer is set equal to the local-address used on the session (or to the router ID if the NLRI is IPv6 and there is no IPv6 local address to use). This is independent of the route origin (EBGP, IBGP or redistributed direct/static/aggregate route). When set to false, normal BGP rules from RFC 4271 apply.
Configurable	True

peer-as *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) peer-as <i>number</i>
Tree	peer-as
Description	The autonomous system number expected from the peer A configured session with a peer does not come up if this value does not match the AS value reported by the peer in its OPEN message.
Range	1 to 4294967295
Configurable	True

peer-group *reference*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) peer-group <i>reference</i>
Tree	peer-group
Description	A reference to the peer-group template to use for this BGP session This is not immutable.
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Configurable	True

received-afi-safi *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-afi-safi <i>keyword</i>
Tree	received-afi-safi
Description	List of multiprotocol BGP address families supported by the peer, derived from the AFI/SAFI list in the MP-BGP capability received by the local routing device from the peer
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	False

received-capabilities *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-capabilities <i>keyword</i>
Tree	received-capabilities
Description	List of BGP capabilities received by the local routing device from the peer
Options	<ul style="list-style-type: none">• MP_BGP

- ROUTE_REFRESH
- EXT_NH_ENCODING
- GRACEFUL_RESTART
- 4-OCTET_ASN
- ORF_SEND_EXCOMM
- ORF_RECEIVE_EXCOMM
- ADD_PATH
- LONG_LIVED_GR

Configurable False

received-end-of-rib *keyword*

Context **network-instance name** *string protocols bgp neighbor peer-address (ipv4-address | ipv6-address)* **received-end-of-rib** *keyword*

Tree **received-end-of-rib**

Description List of address families for which the peer has signaled the End of RIB marker

Options

- ipv4-unicast
- ipv6-unicast

Configurable False

received-messages

Context **network-instance name** *string protocols bgp neighbor peer-address (ipv4-address | ipv6-address)* **received-messages**

Tree **received-messages**

Description Container for state information about BGP messages received from the peer.

Configurable False

keepalives *number*

Context **network-instance name** *string protocols bgp neighbor peer-address (ipv4-address | ipv6-address)* **received-messages keepalives** *number*

Tree **keepalives**

Description Number of BGP KEEPALIVE messages received from the peer over the lifetime of its configuration or since the last clear.

Default 0

Configurable False

last-notification-time *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-messages last-notification-time <i>string</i>
Tree	last-notification-time
Description	The timestamp when the last NOTIFICATION was received from this peer.
Configurable	False

last-update-time *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-messages last-update-time <i>string</i>
Tree	last-update-time
Description	The timestamp when the last UPDATE was received from this peer.
Configurable	False

malformed-updates *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-messages malformed-updates <i>number</i>
Tree	malformed-updates
Description	Number of BGP UPDATE messages received from the peer that were malformed but recoverable through treat-as-withdraw or attribute-discard (i.e. without session reset)
Default	0
Configurable	False

notifications *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-messages notifications <i>number</i>
Tree	notifications
Description	Number of BGP NOTIFICATION messages received from the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

opens *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> received-messages opens <i>number</i>
Tree	opens
Description	Number of BGP OPEN messages received from the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

queue-depth *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> received-messages queue-depth <i>number</i>
Tree	queue-depth
Description	The number of messages received from the peer currently queued.
Configurable	False

route-refresh *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> received-messages route-refresh <i>number</i>
Tree	route-refresh
Description	Number of BGP ROUTE_REFRESH messages received from the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

total-messages *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> received-messages total-messages <i>number</i>
Tree	total-messages
Description	Total number of BGP messages received from the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

total-non-updates *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-messages total-non-updates <i>number</i>
Tree	total-non-updates
Description	Number of BGP NON UPDATE messages received from the peer over the lifetime of its configuration or since the last clear.
Configurable	False

total-updates *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) received-messages total-updates <i>number</i>
Tree	total-updates
Description	Number of BGP UPDATE messages received from the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

route-reflector

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) route-reflector
Tree	route-reflector
Description	Container with route reflection configuration options.
Configurable	True

client *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) route-reflector client <i>boolean</i>
Tree	client
Description	When this is set to true this BGP session is considered an RR client.
Configurable	True

cluster-id *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) route-reflector cluster-id <i>string</i>
Tree	cluster-id
Description	The cluster-id to insert into the CLUSTER_LIST attribute when reflecting routes received by or sent to this client. The default is inherited from group or instance level configuration.
Configurable	True

send-community

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-community
Tree	send-community
Description	Options for controlling the sending of BGP communities to the peer
Configurable	True

large *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-community large <i>boolean</i>
Tree	large
Description	The false setting causes BGP to strip all large (12 byte) BGP communities from all outbound routes advertised to the peer
Configurable	True

standard *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-community standard <i>boolean</i>
Tree	standard
Description	The false setting causes BGP to strip all standard (4 byte) communities from all outbound routes advertised to the peer
Configurable	True

send-default-route

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-default-route
Tree	send-default-route
Description	Options for controlling the generation of default routes towards the peer
Configurable	True

export-policy *reference*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-default-route export-policy <i>reference</i>
Tree	export-policy
Description	The name of a policy that should be applied to the advertised default routes, in order to set their attributes to non-default values Only the default-action of this policy is parsed and applied.
Reference	routing-policy policy name <i>string</i>
Configurable	True

ipv4-unicast *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-default-route ipv4-unicast <i>boolean</i>
Tree	ipv4-unicast
Description	Enables the sending of a synthetically generated default IPv4 route [0/0] to the peer
Configurable	True

ipv6-unicast *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) send-default-route ipv6-unicast <i>boolean</i>
Tree	ipv6-unicast
Description	Enables the sending of a synthetically generated default IPv6 route [::/0] to the peer
Configurable	True

sent-end-of-rib *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-end-of-rib <i>keyword</i>
Tree	sent-end-of-rib
Description	List of address families for which this router sent the peer an End of RIB marker
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	False

sent-messages

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-messages
Tree	sent-messages
Description	Container for state information about BGP messages sent to the peer.
Configurable	False

keepalives *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-messages keepalives <i>number</i>
Tree	keepalives
Description	Number of BGP KEEPALIVE messages sent to the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

last-notification-time *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-messages last-notification-time <i>string</i>
Tree	last-notification-time
Description	The timestamp when the last NOTIFICATION was sent to this peer.
Configurable	False

notifications *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> sent-messages notifications <i>number</i>
Tree	notifications
Description	Number of BGP NOTIFICATION messages sent to the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

opens *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> sent-messages opens <i>number</i>
Tree	opens
Description	Number of BGP OPEN messages sent to the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

queue-depth *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> sent-messages queue-depth <i>number</i>
Tree	queue-depth
Description	The number of messages queued to be sent to the peer.
Configurable	False

route-refresh *number*

Context	network-instance name <i>string protocols bgp neighbor peer-address (ipv4-address ipv6-address)</i> sent-messages route-refresh <i>number</i>
Tree	route-refresh
Description	Number of BGP ROUTE_REFRESH messages sent to the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

total-messages *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-messages total-messages <i>number</i>
Tree	total-messages
Description	Total number of BGP messages sent to the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

total-non-updates *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-messages total-non-updates <i>number</i>
Tree	total-non-updates
Description	Number of BGP NON UPDATE messages sent to the peer over the lifetime of its configuration or since the last clear.
Configurable	False

total-updates *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) sent-messages total-updates <i>number</i>
Tree	total-updates
Description	Number of BGP UPDATE messages sent to the peer over the lifetime of its configuration or since the last clear.
Default	0
Configurable	False

session-state *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) session-state <i>keyword</i>
Tree	session-state
Description	Current state of the session
Options	<ul style="list-style-type: none">• idle• connect• active• opensent• openconfirm

- established
- Configurable False

slow-peer *keyword*

- Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **slow-peer** *keyword*
- Tree **slow-peer**
- Description Set to 'yes' if, after the last BGP restart, the session was in a lesser state than established when the min-wait-to-advertise timer expired
Set to unknown if the min-wait-to-advertise time has not yet elapsed.
- Options
 - yes
 - no
 - unknown
- Configurable False

timers

- Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **timers**
- Tree **timers**
- Description Timer type
- Configurable True

connect-retry *number*

- Context **network-instance name** *string* **protocols bgp neighbor peer-address** (*ipv4-address | ipv6-address*) **timers connect-retry** *number*
- Tree **connect-retry**
- Description The time interval in seconds between successive attempts to establish a session with a peer
- Range 1 to 65535
- Units seconds
- Configurable True

hold-time *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) timers hold-time <i>number</i>
Tree	hold-time
Description	The hold-time interval in seconds that the router proposes to the peer in its OPEN message The actual in-use hold-time is negotiated to the lowest value proposed by the two peers. A negotiated value of 0 suppresses the sending of keepalives by both peers.
Range	0 3 to 65535
Units	seconds
Configurable	True

keepalive-interval *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) timers keepalive-interval <i>number</i>
Tree	keepalive-interval
Description	The interval in seconds between successive keepalive messages sent to the peer The period between one keepalive message and the next is the minimum of this configured (or inherited) value and 1/3 of the negotiated hold-time duration. A value of 0 suppresses the sending of keepalives to the peer.
Range	0 to 21845
Units	seconds
Configurable	True

minimum-advertisement-interval *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) timers minimum-advertisement-interval <i>number</i>
Tree	minimum-advertisement-interval
Description	The value assigned to the MinRouteAdvertisementIntervalTimer of RFC 4271, for both EBGp and IBGP sessions Each session runs its own independent timer and the timer affects both route advertisements and route withdrawals, regardless of address family. For route withdrawals only, this timer is bypassed if rapid-withdrawal is set to true.
Range	1 to 255
Units	seconds
Configurable	True

negotiated-hold-time *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) timers negotiated-hold-time <i>number</i>
Tree	negotiated-hold-time
Description	The operational hold-time It is negotiated to the lowest value proposed by the two peers. A negotiated value of 0 suppresses the sending of keepalives by both peers.
Configurable	False

negotiated-keepalive-interval *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) timers negotiated-keepalive-interval <i>number</i>
Tree	negotiated-keepalive-interval
Description	The operational keepalive interval It is the minimum of the configured value and 1/3 of the negotiated-hold-time. A value of 0 suppresses the sending of keepalives to the peer.
Configurable	False

next-connect-retry-time *string*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) timers next-connect-retry-time <i>string</i>
Tree	next-connect-retry-time
Description	The time when the next connect retry attempt will occur
Configurable	False

trace-options

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) trace-options
Tree	trace-options
Description	Debug traceoptions for BGP
Configurable	True

flag name *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) trace-options flag name <i>keyword</i>
Tree	flag
Description	Tracing parameters
Configurable	True

name *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) trace-options flag name <i>keyword</i>
Description	
Options	<ul style="list-style-type: none">• events Trace all BGP events.• packets Trace all BGP protocol packets.• open Trace BGP open packets.• keepalive Trace BGP keepalive packets.• graceful-restart Trace Graceful Restart events.• timers Trace routing protocol timer processing.• route Trace BGP route table manager.• notification Trace Bgp notification.• socket Trace socket info.• update Trace update info.
Configurable	True

modifier *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) trace-options flag name <i>keyword</i> modifier <i>keyword</i>
Tree	modifier
Description	
Options	<ul style="list-style-type: none">• detail To enable detailed tracing. Includes both received and sent packets.• receive To enable tracing for the packets which are received.• send To enable tracing for the sent packets.
Configurable	True

transport

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) transport
Tree	transport
Description	
Configurable	True

local-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) transport local-address (<i>ipv4-address ipv6-address</i>)
Tree	local-address
Description	The local TCP endpoint of used for the BGP session This also the source address for next-hop-self, if it applies. The local-address can be specified as an IP address that is resolvable to a local interface or else it can refer to a subinterface directly, by name
Configurable	True

local-port *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) transport local-port <i>number</i>
Tree	local-port
Description	Local TCP port used for the TCP connection to the peer
Configurable	False

passive-mode *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) transport passive-mode <i>boolean</i>
Tree	passive-mode
Description	The true setting causes BGP to wait for the peer to initiate the TCP connection The false setting causes BGP to initiate a TCP connection whenever the BGP session is started or restarted.
Configurable	True

remote-port *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) transport remote-port <i>number</i>
Tree	remote-port
Description	Remote TCP port used by the peer for its TCP connection to the local router
Configurable	False

tcp-mss *number*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) transport tcp-mss <i>number</i>
Tree	tcp-mss
Description	The maximum segment size for the BGP TCP session If the configured tcp-mss value is higher than the discovered path MTU it has no effect and the path MTU is used as the operational TCP MSS.
Range	536 to 9446
Units	bytes
Configurable	True

under-maintenance *boolean*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) under-maintenance <i>boolean</i>
Tree	under-maintenance
Description	State field to determine if this bgp neighbor is in maintenance mode.
Configurable	False

oper-state *keyword*

Context	network-instance name <i>string</i> protocols bgp oper-state <i>keyword</i>
Tree	oper-state
Description	
Options	<ul style="list-style-type: none">• up Operational state of BGP is up.• down Operational state of BGP is down.
Configurable	False

preference

Context	network-instance name <i>string</i> protocols bgp preference
Tree	preference
Description	Options for controlling the route table preference of BGP routes
Configurable	True

ebgp *number*

Context	network-instance name <i>string</i> protocols bgp preference ebgp <i>number</i>
Tree	ebgp
Description	The default route table preference for all EBGp learned routes BGP import policies can override this preference value on a route by route basis.
Default	170
Configurable	True

ibgp number

Context	network-instance name <i>string</i> protocols bgp preference ibgp number
Tree	ibgp
Description	The default route table preference for all IBGP learned routes BGP import policies can override this preference value on a route by route basis.
Default	170
Configurable	True

route-advertisement

Context	network-instance name <i>string</i> protocols bgp route-advertisement
Tree	route-advertisement
Description	Options for controlling route advertisement behavior
Configurable	True

rapid-withdrawal *boolean*

Context	network-instance name <i>string</i> protocols bgp route-advertisement rapid-withdrawal <i>boolean</i>
Tree	rapid-withdrawal
Description	The true setting enables rapid-withdraw towards BGP peers If there is only one BGP route for an NLRI in BGP RIB, and this route is withdrawn or becomes invalid, rapid-withdraw causes BGP to immediately send a withdrawal of the BGP route even if the min-route-advertisement timer has not expired.
Default	false
Configurable	True

wait-for-fib-install *boolean*

Context	network-instance name <i>string</i> protocols bgp route-advertisement wait-for-fib-install <i>boolean</i>
Tree	wait-for-fib-install
Description	The true setting causes BGP to NOT advertise initial reachability to a prefix, or a change of reachability to a prefix, until it receives acknowledgment from FIB manager that the route change has been applied Does not apply to route withdrawals.
Default	true
Configurable	True

route-reflector

Context	network-instance name <i>string</i> protocols bgp route-reflector
Tree	route-reflector
Description	Container with route reflection configuration options.
Configurable	True

client *boolean*

Context	network-instance name <i>string</i> protocols bgp route-reflector client <i>boolean</i>
Tree	client
Description	When this is set to true all configured and dynamic sessions of the BGP instance are considered RR clients, subject to overrides at more specific levels of configuration.
Default	false
Configurable	True

cluster-id *string*

Context	network-instance name <i>string</i> protocols bgp route-reflector cluster-id <i>string</i>
Tree	cluster-id
Description	The cluster-id to insert into the CLUSTER_LIST attribute when reflecting routes received by or sent to clients in this scope of this container. The default is the router-id.
Configurable	True

router-id *string*

Context	network-instance name <i>string</i> protocols bgp router-id <i>string</i>
Tree	router-id
Description	The BGP identifier used by this BGP instance in all of its OPEN messages Any non-zero value is supported.
Configurable	True

send-community

Context	network-instance name <i>string</i> protocols bgp send-community
Tree	send-community
Description	Options for controlling the sending of BGP communities to all peers
Configurable	True

large *boolean*

Context	network-instance name <i>string</i> protocols bgp send-community large <i>boolean</i>
Tree	large
Description	The false setting causes BGP to strip all large (12 byte) BGP communities from all outbound routes advertised to peers
Default	true
Configurable	True

standard *boolean*

Context	network-instance name <i>string</i> protocols bgp send-community standard <i>boolean</i>
Tree	standard
Description	The false setting causes BGP to strip all standard (4 byte) communities from all outbound routes advertised to peers
Default	true
Configurable	True

statistics

Context	network-instance name <i>string</i> protocols bgp statistics
Tree	statistics
Description	Container for BGP statistics.
Configurable	False

disabled-peers *number*

Context	network-instance name <i>string</i> protocols bgp statistics disabled-peers <i>number</i>
Tree	disabled-peers
Description	The number of configured BGP peers that are administratively disabled
Configurable	False

dynamic-peers *number*

Context	network-instance name <i>string</i> protocols bgp statistics dynamic-peers <i>number</i>
Tree	dynamic-peers
Description	The number of dynamic BGP peers that are currently in the established state, counting sessions resulting from accepted incoming TCP connections and outgoing TCP connections triggered by LLDP auto-discovery
Configurable	False

path-memory *number*

Context	network-instance name <i>string</i> protocols bgp statistics path-memory <i>number</i>
Tree	path-memory
Description	The total number of bytes required to store the path attribute objects used by all received BGP routes
Default	0
Configurable	False

total-active-routes *number*

Context	network-instance name <i>string</i> protocols bgp statistics total-active-routes <i>number</i>
Tree	total-active-routes
Description	The total number of received BGP routes that are active (installed for forwarding), summed across all address families
Default	0
Configurable	False

total-paths *number*

Context	network-instance name <i>string</i> protocols bgp statistics total-paths <i>number</i>
Tree	total-paths
Description	The total number of path attribute objects used by all received BGP routes
Default	0
Configurable	False

total-peers *number*

Context	network-instance name <i>string</i> protocols bgp statistics total-peers <i>number</i>
Tree	total-peers
Description	The total number of configured BGP peers
Configurable	False

total-prefixes *number*

Context	network-instance name <i>string</i> protocols bgp statistics total-prefixes <i>number</i>
Tree	total-prefixes
Description	The total number of unique NLRI contained in all received BGP routes associated with the BGP instance or the peer-group.
Configurable	False

total-received-routes *number*

Context	network-instance name <i>string</i> protocols bgp statistics total-received-routes <i>number</i>
Tree	total-received-routes
Description	The total number of received BGP routes, summed across all address families
Default	0
Configurable	False

up-peers *number*

Context	network-instance name <i>string</i> protocols bgp statistics up-peers <i>number</i>
Tree	up-peers
Description	The number of configured BGP peers that are currently in the established state
Configurable	False

trace-options

Context	network-instance name <i>string</i> protocols bgp trace-options
Tree	trace-options
Description	Debug traceoptions for BGP
Configurable	True

flag name *keyword*

Context	network-instance name <i>string protocols bgp trace-options flag name keyword</i>
Tree	flag
Description	Tracing parameters
Configurable	True

name *keyword*

Context	network-instance name <i>string protocols bgp trace-options flag name keyword</i>
Description	Name
Options	<ul style="list-style-type: none">• events Trace all BGP events.• packets Trace all BGP protocol packets.• open Trace BGP open packets.• keepalive Trace BGP keepalive packets.• graceful-restart Trace Graceful Restart events.• timers Trace routing protocol timer processing.• route Trace BGP route table manager.• notification Trace Bgp notification.• socket Trace socket info.• update Trace update info.
Configurable	True

modifier *keyword*

Context	network-instance name <i>string</i> protocols bgp trace-options flag name <i>keyword</i> modifier <i>keyword</i>
Tree	modifier
Description	
Options	<ul style="list-style-type: none">• detail To enable detailed tracing. Includes both received and sent packets.• receive To enable tracing for the packets which are received.• send To enable tracing for the sent packets.
Configurable	True

transport

Context	network-instance name <i>string</i> protocols bgp transport
Tree	transport
Description	Options related to the TCP transport of BGP sessions
Configurable	True

tcp-mss *number*

Context	network-instance name <i>string</i> protocols bgp transport tcp-mss <i>number</i>
Tree	tcp-mss
Description	The maximum segment size for all BGP TCP sessions If the configured tcp-mss value is higher than the discovered path MTU it has no effect and the path MTU is used as the operational TCP MSS
Range	536 to 9446
Default	1024
Configurable	True

under-maintenance *boolean*

Context	network-instance name <i>string</i> protocols bgp under-maintenance <i>boolean</i>
Tree	under-maintenance
Description	State field to determine if the bgp instance is in maintenance mode.
Configurable	False

isis

Context	network-instance name <i>string</i> protocols isis
Tree	isis
Description	
Configurable	True

instance name *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>
Tree	instance
Description	List of IS-IS protocol instances associated with this network-instance. Only a single instance is supported for now
Configurable	True
Max. Elements	1

name *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>
Description	The name of the IS-IS instance
String Length	1 to 255
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Used to administratively enable or disable the IS-IS instance
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

attached-bit

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> attached-bit
Tree	attached-bit
Description	This container provides option for handling the ATTached bit in L1 LSPs
Configurable	True

ignore *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> attached-bit ignore <i>boolean</i>
Tree	ignore
Description	When set to true, if the attached bit is set on an incoming Level 1 LSP, the local system ignores it. In this case the local system does not set a default route to the L1L2 router advertising the PDU with the attached bit set.
Default	false
Configurable	True

suppress *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> attached-bit suppress <i>boolean</i>
Tree	suppress
Description	When set to true, if the local IS acts as a L1L2 router, then the attached bit is not advertised in locally generated L1 LSPs.
Default	false
Configurable	True

authentication

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication
Tree	authentication
Description	Container for specifying authentication options that apply to the entire IS-IS instance or to an entire level.
Configurable	True

csnp-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication csnp-authentication <i>boolean</i>
Tree	csnp-authentication
Description	When this is enabled, reject all CSNP PDUs that either have a mismatch in authentication-type or authentication-key.
Configurable	True

hello-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication hello-authentication <i>boolean</i>
Tree	hello-authentication
Description	When this is enabled at the instance level, reject all IIH PDUs that either have a mismatch in authentication-type or authentication-key. When this is enabled for a particular level, reject all LAN IIH PDUs associated with that level that have a mismatch in authentication-type or authentication-key.
Configurable	True

keychain *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication keychain <i>reference</i>
Tree	keychain
Description	
Reference	system authentication keychain name <i>string</i>
Configurable	True

psnp-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication psnp-authentication <i>boolean</i>
Tree	psnp-authentication
Description	When this is enabled, reject all PSNP PDUs that either have a mismatch in authentication-type or authentication-key.
Configurable	True

auto-cost

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> auto-cost
Tree	auto-cost
Description	
Configurable	True

reference-bandwidth *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> auto-cost reference-bandwidth <i>number</i>
Tree	reference-bandwidth
Description	<p>Configures the reference bandwidth that provides the basis for interface metrics based on link bandwidth.</p> <p>If the reference bandwidth is defined, then the cost is calculated using the following formula: cost = reference-bandwidth / bandwidth</p> <p>When a large reference-bandwidth value is configured, a metric calculation may result in a value higher than the supported protocol cost value. If this occurs, IS-IS automatically reverts to the maximum configurable cost metric.</p> <p>If the reference bandwidth is not configured then all interfaces have a default metric of 10.</p> <p>Note: To use metrics in excess of 63, wide metrics must be deployed</p>
Range	1 to 100000000
Units	kbps
Configurable	True

export-policy *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> export-policy <i>reference</i>
Tree	export-policy
Description	Apply an export policy to redistribute non-ISIS routes into ISIS
Reference	routing-policy policy name <i>string</i>
Configurable	True

graceful-restart

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> graceful-restart
Tree	graceful-restart
Description	Container for options related to IS-IS graceful restart
Configurable	True

helper-mode *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> graceful-restart helper-mode <i>boolean</i>
Tree	helper-mode
Description	Enable or disable the IS-IS graceful restart helper function When this leaf is set, the local system supports retaining forwarding information during a neighbor router's restart.
Default	false
Configurable	True

inter-level-propagation-policies

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> inter-level-propagation-policies
Tree	inter-level-propagation-policies
Description	Container with options to control the propagation of prefixes between levels
Configurable	True

level1-to-level2

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> inter-level-propagation-policies level1-to-level2
Tree	level1-to-level2
Description	Container with options to control the propagation of prefixes from level 1 to level 2. By default all L1 prefixes are propagated without summarization into L2.
Configurable	True

summary-address **ip-prefix** (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> inter-level-propagation-policies level1-to-level2 summary-address ip-prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	summary-address
Description	List of summarization prefixes
Configurable	True

ip-prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> inter-level-propagation-policies level1-to-level2 summary-address ip-prefix (<i>ipv4-prefix ipv6-prefix</i>)
Description	An IP prefix advertised into L2 that summarizes one or more L1 prefixes and causes them to be suppressed
Configurable	True

route-tag *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> inter-level-propagation-policies level1-to-level2 summary-address ip-prefix (<i>ipv4-prefix ipv6-prefix</i>) route-tag <i>number</i>
Tree	route-tag
Description	Specifies route tag value to assign to the summary route
Range	1 to 4294967295
Configurable	True

interface **interface-name** *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i>
Tree	interface
Description	List of IS-IS interfaces
Configurable	True

interface-name *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i>
Description	Router logical interface name.
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True

adjacency neighbor-system-id *string* **adjacency-level** *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i>
Tree	adjacency
Description	List of adjacencies formed through this interface.
Configurable	False

neighbor-system-id *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i>
Description	The neighbor router's system ID.
String Length	14
Configurable	False

adjacency-level *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i>
Description	The level of the adjacency that is formed.
Configurable	False

down-reason *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> down-reason <i>keyword</i>
Tree	down-reason
Description	The reason why the adjacency is down.
Options	<ul style="list-style-type: none">• 3-way-handshake-failed• address-mismatch

- hold-timer-expired
- area-mismatch
- bad-hello
- bfd-session-down
- interface-down
- interface-level-disabled
- level-changed
- level-mismatch
- mt-topology-changed
- mt-topology-mismatch
- remote-system-id-changed
- isis-protocol-disabled
- unknown

Configurable False

last-up-down-transition *string*

Context **network-instance name** *string* **protocols isis instance name** *string* **interface interface-name** *reference* **adjacency neighbor-system-id** *string* **adjacency-level** *string* **last-up-down-transition** *string*

Tree **last-up-down-transition**

Description The last time when the adjacency entered the up or down state.

Configurable False

neighbor-circuit-type *keyword*

Context **network-instance name** *string* **protocols isis instance name** *string* **interface interface-name** *reference* **adjacency neighbor-system-id** *string* **adjacency-level** *string* **neighbor-circuit-type** *keyword*

Tree **neighbor-circuit-type**

Description The circuit type signalled by the neighbor.

Default L1L2

Options

- L1
This enum describes ISIS level 1
- L2
This enum describes ISIS level 2
- L1L2
This enum describes ISIS level 1-2

Configurable False

neighbor-hostname *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-hostname <i>string</i>
Tree	neighbor-hostname
Description	The hostname of the neighbor, as learned by TLV 137.
Configurable	False

neighbor-ipv4 *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-ipv4 <i>string</i>
Tree	neighbor-ipv4
Description	The IPv4 address of the neighbor.
Configurable	False

neighbor-ipv6 *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-ipv6 <i>string</i>
Tree	neighbor-ipv6
Description	The IPv6 address of the neighbor.
Configurable	False

neighbor-last-restart (*keyword | date-and-time-delta*)

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-last-restart (<i>keyword date-and-time-delta</i>)
Tree	neighbor-last-restart
Description	The last time the neighbor restarted under protection of graceful restart.
Options	<ul style="list-style-type: none">• never
Configurable	False

neighbor-priority *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-priority <i>number</i>
Tree	neighbor-priority
Description	The priority signalled by the neighbor to become the DIS on a LAN
Range	0 to 127
Configurable	False

neighbor-restart-capable *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-restart-capable <i>boolean</i>
Tree	neighbor-restart-capable
Description	Reads true when the neighbor has signalled that it is restart capable.
Configurable	False

neighbor-restart-status *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-restart-status <i>keyword</i>
Tree	neighbor-restart-status
Description	The status of the neighbor with respect to graceful restart
Options	<ul style="list-style-type: none">• not-helping• helping
Configurable	False

neighbor-restarts *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-restarts <i>number</i>
Tree	neighbor-restarts
Description	The number of times the neighbor has restarted under protection of graceful restart.
Configurable	False

neighbor-snpa *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> neighbor-snpa <i>string</i>
Tree	neighbor-snpa
Description	The SNPA of the neighbor.
String Length	0 to 20
Configurable	False

remaining-holdtime *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> remaining-holdtime <i>number</i>
Tree	remaining-holdtime
Description	The time remaining until the hold timer will expire.
Units	seconds
Configurable	False

state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> state <i>keyword</i>
Tree	state
Description	The current state of the adjacency.
Options	<ul style="list-style-type: none">• up This state describes that adjacency is established.• down This state describes that adjacency is NOT established.• init This state describes that adjacency is establishing.• failed This state describes that adjacency is failed.
Configurable	False

up-down-transitions *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> adjacency neighbor-system-id <i>string</i> adjacency-level <i>string</i> up-down-transitions <i>number</i>
Tree	up-down-transitions
Description	The total number of transitions from Up state to a lower state, since the last clear.
Default	0
Configurable	False

admin-state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Used to administratively enable or disable the IS-IS protocol on a routed subinterface
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

authentication

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication
Tree	authentication
Description	Container for specifying authentication options that apply to an interface/level.
Configurable	True

hello-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication hello-authentication <i>boolean</i>
Tree	hello-authentication
Description	When this is enabled at the instance level, reject all IIH PDUs that either have a mismatch in authentication-type or authentication-key. When this is enabled for a particular level, reject all LAN IIH PDUs associated with that level that have a mismatch in authentication-type or authentication-key.
Configurable	True

keychain *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication keychain <i>reference</i>
Tree	keychain
Description	
Reference	system authentication keychain name <i>string</i>
Configurable	True

circuit-id *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> circuit-id <i>number</i>
Tree	circuit-id
Description	The circuit ID assigned by this IS-IS router to its interface.
Configurable	False

circuit-type *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> circuit-type <i>keyword</i>
Tree	circuit-type
Description	Specifies the circuit type as either point-to-point or broadcast
Options	<ul style="list-style-type: none">point-to-point This enum describes a point-to-point interfacebroadcast This enum describes a broadcast interface
Configurable	True

hello-padding *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> hello-padding <i>keyword</i>
Tree	hello-padding
Description	Specifies the use of IS-IS Hello PDU padding on the interface
Default	disable
Options	<ul style="list-style-type: none">strict Strict padding option. Hello padding is done continuously, regardless of adjacency state or interface type.

- loose
Loose padding option. On p2p interfaces hello PDUs are padded from the initial detection of a new neighbor until the adjacency transitions to the INIT state. On broadcast interfaces hello padding is done until there is at least one UP adjacency on the interface.
- adaptive
Adaptive padding option. On p2p interfaces hello PDUs are padded until the sender declares the adjacency to be UP (based on 3-way handshake or the classic algorithm described in ISO 10589. If the p2p neighbor does not support the adjacency state TLV, then padding continues. On broadcast interfaces hello padding is done until there is at least one UP adjacency on the interface.
- disable
This enum disables hello PDU padding

Configurable True

ipv4-unicast

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [ipv4-unicast](#)

Tree [ipv4-unicast](#)

Description

Configurable True

admin-state *keyword*

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [ipv4-unicast admin-state](#) *keyword*

Tree [admin-state](#)

Description When set to true, the interface and level supports IPv4 unicast routing

Default enable

Options

- enable
- disable

Configurable True

enable-bfd *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv4-unicast enable-bfd <i>boolean</i>
Tree	enable-bfd
Description	Enable BFD for IPv4
Default	false
Configurable	True

include-bfd-tlv *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv4-unicast include-bfd-tlv <i>boolean</i>
Tree	include-bfd-tlv
Description	Specifies whether a BFD-enabled TLV is included for IPv4 on this IS-IS interface.
Default	false
Configurable	True

ipv6-unicast

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv6-unicast
Tree	ipv6-unicast
Description	
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	When set to true, the interface and level supports IPv6 unicast routing
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

enable-bfd *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv6-unicast enable-bfd <i>boolean</i>
Tree	enable-bfd
Description	Enable BFD for IPv6
Default	false
Configurable	True

include-bfd-tlv *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv6-unicast include-bfd-tlv <i>boolean</i>
Tree	include-bfd-tlv
Description	Specifies whether a BFD-enabled TLV is included for IPv6 on this IS-IS interface.
Default	false
Configurable	True

level level-number *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i>
Tree	level
Description	List of IS-IS levels supported by this interface
Configurable	True
Max. Elements	2

level-number *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i>
Description	Specifies the IS-IS protocol level to which these attributes are applied.
Range	1 to 2
Configurable	True

authentication

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> authentication
Tree	authentication
Description	Container for specifying authentication options that apply to an interface/level.
Configurable	True

keychain *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> authentication keychain <i>reference</i>
Tree	keychain
Description	
Reference	system authentication keychain name <i>string</i>
Configurable	True

disable *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> disable <i>boolean</i>
Tree	disable
Description	Disable the Level for the interface.
Default	false
Configurable	True

ipv6-unicast-metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> ipv6-unicast-metric <i>number</i>
Tree	ipv6-unicast-metric
Description	Specifies the interface metric associated with the IPv6-unicast multi-topology. The default is based on reference-bandwidth, or else if this is not configured the default is 10.
Range	1 to 16777215
Configurable	True

metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> metric <i>number</i>
Tree	metric
Description	Specifies the interface metric associated with the native routing topology. The default is based on reference-bandwidth, or else if this is not configured the default is 10.
Range	1 to 16777215
Configurable	True

priority *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> priority <i>number</i>
Tree	priority
Description	ISIS neighbor priority for becoming Designated IS (LAN hello PDU only).
Range	0 to 127
Default	64
Configurable	True

timers

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> timers
Tree	timers
Description	Timer type
Configurable	True

hello-interval *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> timers hello-interval <i>number</i>
Tree	hello-interval
Description	ISIS hello-interval value. The default is 3 seconds on Designated IS interfaces and 9 seconds for non-DIS and p2p interfaces
Range	1 to 20000
Default	9
Units	seconds
Configurable	True

hello-multiplier *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> level level-number <i>number</i> timers hello-multiplier <i>number</i>
Tree	hello-multiplier
Description	<p>ISIS hello-multiplier value.</p> <p>The neighbor hold time is (hello multiplier x hello interval) on non-designated intermediate system broadcast interfaces and point-to-point interfaces and (hello multiplier x hello interval / 3) on designated intermediate system broadcast interfaces.</p> <p>The hold time is the time in which the neighbor expects to receive the next Hello PDU. If the neighbor receives a Hello within this time, the hold time is reset. If the neighbor does not receive a Hello within the hold time, it brings the adjacency down.</p>
Range	2 to 100
Default	3
Configurable	True

oper-state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of the IS-IS interface. This simply tracks the operational state of the subinterface.
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading

Component is currently being upgraded

Configurable False

passive *boolean*

Context **network-instance name** *string* **protocols isis instance name** *string* **interface interface-name** *reference* **passive** *boolean*

Tree **passive**

Description When set to true the interface is configured as a passive interface and does not send IIH PDUs or try to form an adjacency with other routers.

Default false

Configurable True

timers

Context **network-instance name** *string* **protocols isis instance name** *string* **interface interface-name** *reference* **timers**

Tree **timers**

Description Timer type

Configurable True

csnp-interval *number*

Context **network-instance name** *string* **protocols isis instance name** *string* **interface interface-name** *reference* **timers csnp-interval** *number*

Tree **csnp-interval**

Description The interval, specified in seconds, at which periodic CSNP packets should be transmitted by the local IS on this interface.

Range 1 to 300

Default 10

Units seconds

Configurable True

lsp-pacing-interval *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> timers lsp-pacing-interval <i>number</i>
Tree	lsp-pacing-interval
Description	<p>Controls the interval between (bursts of) LSPs sent from the interface. The interval applies to all LSPs: LSPs generated by the router, and LSPs received from other routers and re-flooded.</p> <p>The burst interval is 100 ms if the lsp-pacing-interval < 100 ms and otherwise it is 1 second. For example, if the lsp-pacing-interval is 2 ms, at most 50 LSPs are sent every 100 ms. On the other hand, if the lsp-pacing-interval is 100 ms, at most 10 LSPs are sent every 1 second.</p> <p>If a value of 0 is configured, no LSPs are sent from the interface.</p> <p>The default pacing interval of 100 milliseconds means that a maximum of 10 LSPs are sent in a burst every second.</p>
Range	0 to 100000
Default	100
Units	milliseconds
Configurable	True

trace-options

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> trace-options
Tree	trace-options
Description	Interface level debug trace options for IS-IS
Configurable	True

trace *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> trace-options trace <i>keyword</i>
Tree	trace
Description	List of tracing options
Options	<ul style="list-style-type: none"> • adjacencies • packets-all • packets-p2p-hello • packets-l1-hello • packets-l2-hello • packets-l1-psnp • packets-l2-psnp

- packets-l1-csnp
- packets-l2-csnp
- packets-l1-lsp
- packets-l2-lsp

Configurable True

ipv4-unicast

Context **network-instance name** *string* **protocols isis instance name** *string* **ipv4-unicast**

Tree **ipv4-unicast**

Description Enables/disables IPv4 routing in this ISIS instance.

Configurable True

admin-state *keyword*

Context **network-instance name** *string* **protocols isis instance name** *string* **ipv4-unicast admin-state** *keyword*

Tree **admin-state**

Description When set to true, the IS-IS instance supports IPv4 unicast routing

Default enable

Options

- enable
- disable

Configurable True

ipv6-unicast

Context **network-instance name** *string* **protocols isis instance name** *string* **ipv6-unicast**

Tree **ipv6-unicast**

Description Enables/disables IPv6 routing in this ISIS instance.

Configurable True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Description	When set to true, the IS-IS instance supports IPv6 unicast routing
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

multi-topology *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ipv6-unicast multi-topology <i>boolean</i>
Tree	multi-topology
Description	When set to true, IS-IS multi-topology TLVs are used for IPv6 routing and support for native IPv6 TLVs is disabled.
Default	false
Configurable	True

level level-number *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i>
Tree	level
Description	List of IS-IS levels supported by this IS (router)
Configurable	True
Max. Elements	2

level-number *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i>
Description	Specifies the IS-IS protocol level to which these attributes are applied.
Range	1 to 2
Configurable	True

authentication

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number number authentication
Tree	authentication
Description	Container for specifying authentication options that apply to the entire IS-IS instance or to an entire level.
Configurable	True

csnp-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number number authentication csnp-authentication <i>boolean</i>
Tree	csnp-authentication
Description	When this is enabled, reject all CSNP PDUs that either have a mismatch in authentication-type or authentication-key.
Configurable	True

hello-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number number authentication hello-authentication <i>boolean</i>
Tree	hello-authentication
Description	When this is enabled at the instance level, reject all IIH PDUs that either have a mismatch in authentication-type or authentication-key. When this is enabled for a particular level, reject all LAN IIH PDUs associated with that level that have a mismatch in authentication-type or authentication-key.
Configurable	True

keychain *reference*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number number authentication keychain <i>reference</i>
Tree	keychain
Description	
Reference	system authentication keychain name <i>string</i>
Configurable	True

psnp-authentication *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication psnp-authentication <i>boolean</i>
Tree	psnp-authentication
Description	When this is enabled, reject all PSNP PDUs that either have a mismatch in authentication-type or authentication-key.
Configurable	True

metric-style *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> metric-style <i>keyword</i>
Tree	metric-style
Description	Specifies the metric style to be wide or narrow for the level
Default	wide
Options	<ul style="list-style-type: none">• narrow This enum describes narrow metric style• wide This enum describes wide metric style
Configurable	True

route-preference

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> route-preference
Tree	route-preference
Description	Specify the route preference (admin distance) for IP routes associated with the level
Configurable	True

external *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> route-preference external <i>number</i>
Tree	external
Description	Specify the route preference of external routes carried in this level. By default the route preference of external L1 routes is 160. By default the route preference of external L2 routes is 165.
Range	1 to 255
Configurable	True

internal *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> route-preference internal <i>number</i>
Tree	internal
Description	Specify the route preference of internal routes carried in this level. By default the route preference of internal L1 routes is 15. By default the route preference of internal L2 routes is 18.
Range	1 to 255
Configurable	True

trace-options

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> trace-options
Tree	trace-options
Description	Level debug trace options for IS-IS
Configurable	True

trace *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> trace-options trace <i>keyword</i>
Tree	trace
Description	List of tracing options
Options	<ul style="list-style-type: none">• adjacencies• isdb• routes

	<ul style="list-style-type: none">• spf
Configurable	True

level-capability *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-capability <i>keyword</i>
Tree	level-capability
Description	The level-capability of the intermediate system (router)
Default	L2
Options	<ul style="list-style-type: none">• L1 This enum describes ISIS level 1• L2 This enum describes ISIS level 2• L1L2 This enum describes ISIS level 1-2
Configurable	True

level-database **level-number** *number* **lsp-id** *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i>
Tree	level-database
Description	Link State database
Configurable	False

level-number *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i>
Description	Specifies the IS-IS protocol level to which these attributes are applied.
Range	1 to 2
Configurable	False

lsp-id *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i>
Description	The value specifies the LSP Id and is given in the format as 6 octets of adjacency system-id followed by 1 octet Lan-ID and 1 octet LSP Number.
String Length	20
Configurable	False

attributes

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> attributes
Tree	attributes
Description	
Configurable	False

attached *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> attributes attached <i>boolean</i>
Tree	attached
Description	Set to true in the L1 LSP when the IS has a Level 2 adjacency.
Configurable	False

level1-is-type *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> attributes level1-is-type <i>boolean</i>
Tree	level1-is-type
Description	Set to true when the router participates in L1
Configurable	False

level2-is-type *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> attributes level2-is-type <i>boolean</i>
Tree	level2-is-type
Description	Set to true when the router participates in L2
Configurable	False

overload *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> attributes overload <i>boolean</i>
Tree	overload
Description	Set to true when the IS is in overload state and should be avoided for transit.
Configurable	False

checksum *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> checksum <i>string</i>
Tree	checksum
Description	The value indicates the checksum of contents of LSP from the SourceID field in the LSP till the end. The checksum is computed using the Fletcher checksum algorithm.
Configurable	False

defined-tlvs

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs
Tree	defined-tlvs
Description	List of defined TLV-s contained in LSP.
Configurable	False

area-addresses *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs area-addresses <i>string</i>
Tree	area-addresses
Description	Each item represents an area address advertised by the LSP.
String Length	2 to 38
Configurable	False

authentication

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs authentication
Tree	authentication
Description	Authentication TLV. TLV type = 10
Configurable	False

auth-data *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs authentication auth-data <i>string</i>
Tree	auth-data
Description	The authentication data
Configurable	False

auth-type *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs authentication auth-type <i>keyword</i>
Tree	auth-type
Description	The authentication type
Options	<ul style="list-style-type: none">• cleartext• crypto• hmac-md5
Configurable	False

extended-ipv4-reachability **ipv4-prefix** *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-ipv4-reachability ipv4-prefix <i>string</i>
Tree	extended-ipv4-reachability
Description	TLV specifying extended IPv4 Reachability information in the LSP. TLV type = 135
Configurable	False

ipv4-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-ipv4-reachability ipv4-prefix <i>string</i>
Description	An IPv4 prefix that is reachable to the router.
Configurable	False

down *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-ipv4-reachability ipv4-prefix <i>string</i> down <i>boolean</i>
Tree	down
Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
Configurable	False

metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-ipv4-reachability ipv4-prefix <i>string</i> metric <i>number</i>
Tree	metric
Description	The default metric to reach the IPv4 prefix.
Range	0 to 16777215
Configurable	False

extended-is-reachability neighbor *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-is-reachability neighbor <i>string</i>
Tree	extended-is-reachability
Description	Each TLV encodes the identity of an adjacent IS neighbor. TLV type = 22
Configurable	False

neighbor *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-is-reachability neighbor <i>string</i>
Description	An adjacent IS neighbor
String Length	17
Configurable	False

default-metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-is-reachability neighbor <i>string</i> default-metric <i>number</i>
Tree	default-metric
Description	The default metric to reach this adjacent neighbor.
Range	0 to 16777215
Configurable	False

sub-tlvs

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-is-reachability neighbor <i>string</i> sub-tlvs
Tree	sub-tlvs
Description	SubTLVs of TLV 22
Configurable	False

ipv4-interface-address *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs extended-is-reachability neighbor <i>string</i> sub-tlvs ipv4-interface-address <i>string</i>
Tree	ipv4-interface-address
Description	The IPv4 address associated with the neighbor.
Configurable	False

hostname *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs hostname <i>string</i>
Tree	hostname
Description	Host name that advertised this LSP.
Configurable	False

ipv4-external-reachability [ipv4-prefix](#) *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-external-reachability ipv4-prefix <i>string</i>
Tree	ipv4-external-reachability
Description	TLV specifying external IPv4 Reachability information in the LSP. External reachability is typically routing information learned from another protocol. TLV type = 130
Configurable	False

ipv4-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-external-reachability ipv4-prefix <i>string</i>
Description	An IPv4 prefix that is reachable to the router.
Configurable	False

default-metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-external-reachability ipv4-prefix <i>string</i> default-metric <i>number</i>
Tree	default-metric
Description	The default metric to reach the IPv4 prefix.
Range	0 to 63
Configurable	False

default-metric-type *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-external-reachability ipv4-prefix <i>string</i> default-metric-type <i>keyword</i>
Tree	default-metric-type
Description	The default metric type: internal or external.
Options	<ul style="list-style-type: none">• internal This enum describes internal route type• external This enum describes external route type
Configurable	False

down *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-external-reachability ipv4-prefix <i>string</i> down <i>boolean</i>
Tree	down
Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
Configurable	False

ipv4-interface-addresses (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-interface-addresses (<i>ipv4-address ipv6-address</i>)
Tree	ipv4-interface-addresses
Description	Each item represents an IPv4 address configured on an interface in this IS-IS instance.
Configurable	False

ipv4-internal-reachability **ipv4-prefix** *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-internal-reachability ipv4-prefix <i>string</i>
Tree	ipv4-internal-reachability
Description	TLV specifying internal IPv4 Reachability information in the LSP. TLV type = 128
Configurable	False

ipv4-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-internal-reachability ipv4-prefix <i>string</i>
Description	An IPv4 prefix that is reachable to the router.
Configurable	False

default-metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-internal-reachability ipv4-prefix <i>string</i> default-metric <i>number</i>
Tree	default-metric
Description	The default metric to reach the IPv4 prefix.
Range	0 to 63
Configurable	False

default-metric-type *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-internal-reachability ipv4-prefix <i>string</i> default-metric-type <i>keyword</i>
Tree	default-metric-type
Description	The default metric type: internal or external.
Options	<ul style="list-style-type: none">• internal This enum describes internal route type• external This enum describes external route type
Configurable	False

down *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv4-internal-reachability ipv4-prefix <i>string</i> down <i>boolean</i>
Tree	down
Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
Configurable	False

ipv6-interface-addresses (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv6-interface-addresses (<i>ipv4-address ipv6-address</i>)
Tree	ipv6-interface-addresses
Description	Each item represents an IPv6 address configured on an interface in this IS-IS instance.
Configurable	False

ipv6-reachability ipv6-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv6-reachability ipv6-prefix <i>string</i>
Tree	ipv6-reachability
Description	TLV specifying IPv6 Reachability information in the LSP. TLV type = 236
Configurable	False

ipv6-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv6-reachability ipv6-prefix <i>string</i>
Description	An IPv6 prefix that is reachable to the router.
Configurable	False

down *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv6-reachability ipv6-prefix <i>string</i> down <i>boolean</i>
Tree	down
Description	Reads true when the IPv6 prefix was leaked down from Level2 to Level1.
Configurable	False

external *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv6-reachability ipv6-prefix <i>string</i> external <i>boolean</i>
Tree	external
Description	Reads true when the IPv6 prefix reachability is external (learned from another protocol).
Configurable	False

metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs ipv6-reachability ipv6-prefix <i>string</i> metric <i>number</i>
Tree	metric
Description	The metric to reach this IPv6 prefix.
Range	0 to 16777215
Configurable	False

is-reachability neighbor *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs is-reachability neighbor <i>string</i>
Tree	is-reachability
Description	Each TLV encodes the identity of an adjacent IS neighbor. TLV type = 2
Configurable	False

neighbor *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs is-reachability neighbor <i>string</i>
Description	An adjacent IS neighbor
String Length	17
Configurable	False

default-metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs is-reachability neighbor <i>string</i> default-metric <i>number</i>
Tree	default-metric
Description	The default metric to reach this adjacent neighbor.
Range	0 to 63
Configurable	False

default-metric-type *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs is-reachability neighbor <i>string</i> default-metric-type <i>keyword</i>
Tree	default-metric-type
Description	The default metric type: internal or external.
Options	<ul style="list-style-type: none">• internal• external
Configurable	False

mt-ipv4-reachability **ipv4-prefix** *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv4-reachability ipv4-prefix <i>string</i>
Tree	mt-ipv4-reachability
Description	TLV specifying multi-topology IPv4 reachability information in the LSP. TLV type = 235
Configurable	False

ipv4-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv4-reachability ipv4-prefix <i>string</i>
Description	An IPv4 prefix that is reachable to the router.
Configurable	False

down *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv4-reachability ipv4-prefix <i>string</i> down <i>boolean</i>
Tree	down
Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
Configurable	False

metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv4-reachability ipv4-prefix <i>string</i> metric <i>number</i>
Tree	metric
Description	The default metric to reach the IPv4 prefix.
Range	1 to 16777215
Configurable	False

mt-id *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv4-reachability ipv4-prefix <i>string</i> mt-id <i>number</i>
Tree	mt-id
Description	A multi-topology ID.
Range	0 to 4095
Configurable	False

mt-ipv6-reachability **ipv6-prefix** *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv6-reachability ipv6-prefix <i>string</i>
Tree	mt-ipv6-reachability
Description	TLV specifying IPv6 Reachability information in the LSP. TLV type = 237
Configurable	False

ipv6-prefix *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv6-reachability ipv6-prefix <i>string</i>
Description	An IPv6 prefix that is reachable to the router.
Configurable	False

down *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv6-reachability ipv6-prefix <i>string</i> down <i>boolean</i>
Tree	down
Description	Reads true when the IPv6 prefix was leaked down from Level2 to Level1.
Configurable	False

external *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv6-reachability ipv6-prefix <i>string</i> external <i>boolean</i>
Tree	external
Description	Reads true when the IPv6 prefix reachability is external (learned from another protocol).
Configurable	False

metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv6-reachability ipv6-prefix <i>string</i> metric <i>number</i>
Tree	metric
Description	The metric to reach this IPv6 prefix.
Range	1 to 16777215
Configurable	False

mt-id *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-ipv6-reachability ipv6-prefix <i>string</i> mt-id <i>number</i>
Tree	mt-id
Description	A multi-topology ID.
Range	0 to 4095
Configurable	False

mt-is-reachability [neighbor](#) *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-is-reachability neighbor <i>string</i>
Tree	mt-is-reachability
Description	Each TLV encodes the identity of an adjacent IS neighbor in a specific topology. TLV type = 222
Configurable	False

neighbor *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-is-reachability neighbor <i>string</i>
Description	An adjacent IS neighbor
String Length	17
Configurable	False

default-metric *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-is-reachability neighbor <i>string</i> default-metric <i>number</i>
Tree	default-metric
Description	The default metric to reach this adjacent neighbor.
Range	1 to 16777215
Configurable	False

mt-id *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs mt-is-reachability neighbor <i>string</i> mt-id <i>number</i>
Tree	mt-id
Description	A multi-topology ID.
Range	0 to 4095
Configurable	False

multi-topology

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs multi-topology
Tree	multi-topology
Description	The Multi-Topology TLV, type 229.
Configurable	False

topology **mt-id** *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs multi-topology topology mt-id <i>number</i>
Tree	topology
Description	The list of multi-topology IDs that the router is participating in
Configurable	False

mt-id *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs multi-topology topology mt-id <i>number</i>
Description	A multi-topology ID.
Range	0 to 4095
Configurable	False

attached *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs multi-topology topology mt-id <i>number</i> attached <i>boolean</i>
Tree	attached
Description	Reads true when the topology is attached to Level 2
Configurable	False

overload *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs multi-topology topology mt-id <i>number</i> overload <i>boolean</i>
Tree	overload
Description	Reads true when the topology is in overload state.
Configurable	False

nlpid *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs nlpid <i>keyword</i>
Tree	nlpid
Description	Each item represents a network layer protocol supported by the IS-IS Instance.
Options	<ul style="list-style-type: none">• IPv4 NLPID 0xCC corresponding to IPv4• IPv6 NLPID 0x8E corresponding to IPv6• CLNS NLPID 0x81 corresponding to CLNS
Configurable	False

purge-oi *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> defined-tlvs purge-oi <i>string</i>
Tree	purge-oi
Description	This indicates System ID that originated a purge.
String Length	14
Configurable	False

maximum-area-addresses *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> maximum-area-addresses <i>number</i>
Tree	maximum-area-addresses
Description	The value indicates the maximum number of areas supported by the originator of the LSP. A value of 0 indicates a default of 3 areas.
Configurable	False

pdu-length *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> pdu-length <i>number</i>
Tree	pdu-length
Description	The value indicates the PDU length for instance LSPs, CSNPs OR PSNPs at both IS-IS protocol levels i.e. L1 and L2 as maintained in the database.
Configurable	False

pdu-type *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> pdu-type <i>number</i>
Tree	pdu-type
Description	The value indicates the PDU type for instance LSPs, CSNPs OR PSNPs at both IS-IS protocol levels i.e. L1 and L2 as maintained in of the object packet-type.
Configurable	False

pkt-version *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> pkt-version <i>number</i>
Tree	pkt-version
Description	The value indicates the version of the ISIS protocol that has generated the Packet.
Configurable	False

remaining-lifetime *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> remaining-lifetime <i>number</i>
Tree	remaining-lifetime
Description	The value indicates the Remaining lifetime of this LSP and is a decrementing counter that decrements in seconds starting from the value as received in the LSP if not self-originated OR from lsp-life-time for self originated LSPs. When the remaining lifetime becomes zero, the contents of the LSP should not be considered for SPF calculation.
Range	0 to 65535
Units	seconds
Configurable	False

sequence-number *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> sequence-number <i>string</i>
Tree	sequence-number
Description	The value indicates the sequence number of an LSP and is a four byte quantity that represents the version of an LSP. The higher the sequence number, the more up to date the information. The sequence number is always incremented by the system that originated the LSP and ensures that there is only one version of that LSP in the entire network.
Configurable	False

system-id-len *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> system-id-len <i>number</i>
Tree	system-id-len
Description	The value indicates the length of the system-id as used by the originator.
Configurable	False

undefined-tlvs *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> undefined-tlvs <i>string</i>
Tree	undefined-tlvs
Description	Undefined TLV-s as contents of the LSP.
String Length	27 to 9190
Configurable	False

version *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level-database level-number <i>number</i> lsp-id <i>string</i> version <i>number</i>
Tree	version
Description	The value indicates the version of the ISIS protocol that has generated the LSP
Configurable	False

max-ecmp-paths *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> max-ecmp-paths <i>number</i>
Tree	max-ecmp-paths
Description	The maximum number of ECMP next-hops to program into the FIB for every IP prefix
Range	1 to 64
Default	1
Configurable	True

net *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> net <i>string</i>
Tree	net
Description	ISIS network entity title (NET)
Configurable	True
Max. Elements	1

oper-state *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The value of the this object indicates the operational state of the destination.
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

oper-system-id *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> oper-system-id <i>string</i>
Tree	oper-system-id
Description	The ID for this instance of the Integrated IS-IS protocol.
String Length	14
Configurable	False

overload

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload
Tree	overload
Description	Specifies isis routing instance behavior regarding overload
Configurable	True

advertise-external *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload advertise-external <i>boolean</i>
Tree	advertise-external
Description	When set to true, external (non-ISIS) routes continue to be advertised when the router is in overload.
Default	false
Configurable	True

advertise-interlevel *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload advertise-interlevel <i>boolean</i>
Tree	advertise-interlevel
Description	When set to true, L1->L2 and L2->L1 inter-level routes continue to be advertised when the router is in overload.
Default	false
Configurable	True

immediate

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload immediate
Tree	immediate
Description	Options for advertising an overloaded state immediately
Configurable	True

max-metric *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload immediate max-metric <i>boolean</i>
Tree	max-metric
Description	When set to true transit links are advertised with a wide metric of 0xfffffe and a narrow metric of 0x3f
Default	false
Configurable	True

set-bit *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload immediate set-bit <i>boolean</i>
Tree	set-bit
Description	When set to true, the Overload bit is set
Default	false
Configurable	True

on-boot

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload on-boot
Tree	on-boot
Description	Options for advertising an overloaded state whenever the IS-IS process restarts
Configurable	True

max-metric *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload on-boot max-metric <i>boolean</i>
Tree	max-metric
Description	When set to true transit links are advertised with a wide metric of 0xfffffe and a narrow metric of 0x3f
Default	false
Configurable	True

set-bit *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload on-boot set-bit <i>boolean</i>
Tree	set-bit
Description	When set to true, the Overload bit is set
Default	false
Configurable	True

timeout *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload on-boot timeout <i>number</i>
Tree	timeout
Description	Specifies the time that the router should remain in overload state after the IS-IS process restarts
Range	60 to 1800
Units	seconds
Configurable	True

poi-tlv *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> poi-tlv <i>boolean</i>
Tree	poi-tlv
Description	When set to true, a TLV is added to purge to record the system ID of the IS generating the purge.
Default	false
Configurable	True

statistics

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics
Tree	statistics
Description	Instance level statistics
Configurable	False

last-partial-spf *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics last-partial-spf <i>string</i>
Tree	last-partial-spf
Description	The elapsed time since the last time a partial SPF run was run on either the L1 or L2 LSDB
Configurable	False

last-spf *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics last-spf <i>string</i>
Tree	last-spf
Description	The elapsed time since the last time a full SPF run was run on either the L1 or L2 LSDB
Configurable	False

partial-spf-runs *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics partial-spf-runs <i>number</i>
Tree	partial-spf-runs
Description	The number of times a partial SPF run has been performed on either the L1 or L2 LSDB since the IS-IS manager restarted
Default	0
Configurable	False

pdu pdu-name *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i>
Tree	pdu
Description	List of PDUs processed by the IS-IS instance since the IS-IS manager restarted
Configurable	False

pdu-name *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i>
Description	The PDU type that was processed
Options	<ul style="list-style-type: none">• LSP Link State PDU• IIH IS-to-IS Hello PDU• CSNP Complete Sequence Number PDU• PSNP Partial Sequence Number PDU• Unknown

Unknown PDU type

Configurable False

dropped *number*

Context **network-instance name** *string* **protocols isis instance name** *string* **statistics pdu pdu-name** *keyword* **dropped** *number*

Tree **dropped**

Description The number of PDUs that were received and dropped

Default 0

Configurable False

processed *number*

Context **network-instance name** *string* **protocols isis instance name** *string* **statistics pdu pdu-name** *keyword* **processed** *number*

Tree **processed**

Description The number of PDUs that were received and processed

Default 0

Configurable False

received *number*

Context **network-instance name** *string* **protocols isis instance name** *string* **statistics pdu pdu-name** *keyword* **received** *number*

Tree **received**

Description The number of PDUs that were received

Default 0

Configurable False

retransmitted *number*

Context **network-instance name** *string* **protocols isis instance name** *string* **statistics pdu pdu-name** *keyword* **retransmitted** *number*

Tree **retransmitted**

Description The number of PDUs that were retransmitted

Default 0

Configurable False

sent *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i> sent <i>number</i>
Tree	sent
Description	The number of PDUs that were transmitted
Default	0
Configurable	False

spf-runs *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics spf-runs <i>number</i>
Tree	spf-runs
Description	The number of times a full SPF run has been performed on either the L1 or L2 LSDB since the IS-IS manager restarted
Default	0
Configurable	False

timers

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers
Tree	timers
Description	Container for IS-IS timers applicable at the instance level
Configurable	True

Isp-generation

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers Isp-generation
Tree	Isp-generation
Description	Container with options for specifying LSP generation timer values
Configurable	True

initial-wait *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers Isp-generation initial-wait <i>number</i>
Tree	initial-wait
Description	Time interval between the detection of topology change and when the new LSP is generated.

	The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

max-wait *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers lsp-generation max-wait <i>number</i>
Tree	max-wait
Description	Specifies the maximum interval between two consecutive generations of an LSP. The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms
Range	10 to 120000
Default	5000
Units	milliseconds
Configurable	True

second-wait *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers lsp-generation second-wait <i>number</i>
Tree	second-wait
Description	Time interval between the the first and second LSP generation. The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

Isp-lifetime *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers Isp-lifetime number
Tree	Isp-lifetime
Description	Time interval in seconds that the LSPs originated by this IS (router) remain valid in the LSDB before they must be refreshed or else they are purged.
Range	350 to 65535
Default	1200
Units	seconds
Configurable	True

Isp-refresh

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers Isp-refresh
Tree	Isp-refresh
Description	Configure LSP refresh timers.
Configurable	True

half-lifetime *boolean*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers Isp-refresh half-lifetime <i>boolean</i>
Tree	half-lifetime
Description	When set to true, the LSP refresh interval is half the Isp-lifetime
Default	true
Configurable	True

interval *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers lsp-refresh interval <i>number</i>
Tree	interval
Description	Time interval in seconds since the last advertisement of its LSP when the router attempts to refresh the LSP. Must not exceed 90% of the lsp-lifetime. This value is ignored when half-lifetime is set to true.
Range	150 to 65535
Default	600
Units	seconds
Configurable	True

spf

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers spf
Tree	spf
Description	Container with options for specifying SPF timer values
Configurable	True

initial-wait *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers spf initial-wait <i>number</i>
Tree	initial-wait
Description	Time interval between the detection of topology change and when the SPF algorithm runs. The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

max-wait *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers spf max-wait <i>number</i>
Tree	max-wait
Description	Specifies the maximum interval between two consecutive SPF calculations in milliseconds.

	The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms
Range	10 to 120000
Default	10000
Units	milliseconds
Configurable	True

second-wait *number*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers spf second-wait <i>number</i>
Tree	second-wait
Description	Time interval between the the first and second SPF run. The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

trace-options

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> trace-options
Tree	trace-options
Description	Instance level debug trace options for IS-IS
Configurable	True

trace *keyword*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> trace-options trace <i>keyword</i>
Tree	trace
Description	List of tracing options
Options	<ul style="list-style-type: none"> • adjacencies • graceful-restart • interfaces • packets-all • packets-p2p-hello

- packets-l1-hello
- packets-l2-hello
- packets-l1-psnp
- packets-l2-psnp
- packets-l1-csnp
- packets-l2-csnp
- packets-l1-lsp
- packets-l2-lsp
- routes
- summary-addresses

Configurable True

transport

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [transport](#)

Tree [transport](#)

Description

Configurable True

lsp-mtu-size *number*

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [transport lsp-mtu-size](#) *number*

Tree [lsp-mtu-size](#)

Description Sets the maximum size of LSPs generated by this router

Range 490 to 9490

Default 1492

Units bytes

Configurable True

linux

Context [network-instance name](#) *string* [protocols linux](#)

Tree [linux](#)

Description

Configurable True

export-neighbors *boolean*

Context	network-instance name <i>string</i> protocols linux export-neighbors <i>boolean</i>
Tree	export-neighbors
Description	Export neighbors to linux routing table
Default	true
Configurable	True

export-routes *boolean*

Context	network-instance name <i>string</i> protocols linux export-routes <i>boolean</i>
Tree	export-routes
Description	Export routes to linux routing table
Default	false
Configurable	True

import-routes *boolean*

Context	network-instance name <i>string</i> protocols linux import-routes <i>boolean</i>
Tree	import-routes
Description	Import routes from linux routing table
Default	false
Configurable	True

ospfv2

Context	network-instance name <i>string</i> protocols ospfv2
Tree	ospfv2
Description	Top-level configuration and operational state for Open Shortest Path First (OSPF) v2
Configurable	True

instance name *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i>
Tree	instance
Description	List of OSPFv2 protocol instances associated with this network-instance. Only a single instance is supported for now
Configurable	True
Max. Elements	1

name *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i>
Description	The name of the OSPFv2 instance
String Length	1 to 255
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Used to administratively enable or disable the OSPF instance
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

advertise-router-capability *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> advertise-router-capability <i>keyword</i>
Tree	advertise-router-capability
Description	Scope to advertise router-capability.
Options	<ul style="list-style-type: none">• false• link• area• as
Configurable	True

area **area-id** *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i>
Tree	area
Description	The OSPFv2 areas within which the local system exists
Configurable	True

area-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i>
Description	the area identifier as a dotted-quad.
Configurable	True

advertise-router-capability *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> advertise-router-capability <i>boolean</i>
Tree	advertise-router-capability
Description	Allow router advertisement capabilities
Default	true
Configurable	True

area-range **ip-prefix-mask** *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> area-range ip-prefix-mask <i>string</i>
Tree	area-range
Description	Enter the area-range context
Configurable	True

ip-prefix-mask *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> area-range ip-prefix-mask <i>string</i>
Description	ip-prefix a.b.c.d (host bits must be 0) mask [0..32]
Configurable	True

advertise *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> area-range ip-prefix-mask <i>string</i> advertise <i>boolean</i>
Tree	advertise
Description	Advertise summarized range of addresses to other areas
Default	true
Configurable	True

blackhole-aggregate *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> blackhole-aggregate <i>boolean</i>
Tree	blackhole-aggregate
Description	Enables the creation of a blackhole for generated aggregates
Configurable	True

export-policy *reference*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> export-policy <i>reference</i>
Tree	export-policy
Description	Apply an export policy to redistribute non-OSPFv2 routes into OSPF
Reference	routing-policy policy name <i>string</i>
Configurable	True

interface [interface-name](#) *reference*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i>
Tree	interface
Description	List of OSPFv2 interfaces
Configurable	True

interface-name *reference*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i>
Description	Router logical interface name.
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Administrative state of the OSPF
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

advertise-router-capability *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> advertise-router-capability <i>boolean</i>
Tree	advertise-router-capability
Description	Allow router advertisement capabilities
Default	true
Configurable	True

advertise-subnet *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> advertise-subnet <i>boolean</i>
Tree	advertise-subnet
Description	Advertise point-to-point interfaces as subnet routes
Default	true
Configurable	True

authentication

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> authentication
Tree	authentication
Description	Container with authentication options that apply to all peers in this peer-group
Configurable	True

keychain *reference*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> authentication keychain <i>reference</i>
Tree	keychain
Description	Reference to a keychain. The keychain type must be tcp-md5 or tcp-ao.
Reference	system authentication keychain name <i>string</i>
Configurable	True

bad-packets

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets
Tree	bad-packets
Description	Bad packets counters
Configurable	False

bad-area *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-area <i>number</i>
Tree	bad-area
Description	The total number of OSPF packets received with an area mismatch since admin-state was last set to 'enabled'.
Configurable	False

bad-auth-type *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-auth-type <i>number</i>
Tree	bad-auth-type
Description	The total number of OSPF packets received with an invalid authorization type since admin-state was last set to 'enabled'.
Configurable	False

bad-checksum *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-checksum <i>number</i>
Tree	bad-checksum
Description	The count of LS-as received with bad checksums.
Configurable	False

bad-dead-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-dead-interval <i>number</i>
Tree	bad-dead-interval
Description	The total number of OSPF packets received where the dead interval given in the packet was not equal to that configured on this interface since admin-state was last set to 'enabled'.
Configurable	False

bad-dest-address *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-dest-address <i>number</i>
Tree	bad-dest-address
Description	The total number of OSPF packets received with the incorrect IP destination address since admin-state was last set to 'enabled'.
Configurable	False

bad-hello-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-hello-interval <i>number</i>
Tree	bad-hello-interval
Description	the value of bad-hello-intervals indicates the total number of OSPF packets received where the hello interval given in packet was not equal to that configured on this interface since admin-state was last set to 'enabled'.
Configurable	False

bad-length *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-length <i>number</i>
Tree	bad-length
Description	The total number of OSPF packets received with a total length not equal to the length given in the packet itself since admin-state was last set to 'enabled'.
Configurable	False

bad-neighbors *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-neighbors <i>number</i>
Tree	bad-neighbors
Description	The total number of OSPF packets received where the neighbor information does not match the information this router has for the neighbor since admin-state was last set to 'enabled'.
Configurable	False

bad-network *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-network <i>number</i>
Tree	bad-network
Description	The total number of OSPF packets received with invalid network or mask since admin-state was last set to 'enabled'.
Configurable	False

bad-options *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-options <i>number</i>
Tree	bad-options
Description	The total number of OSPF packets received with an option that does not match those configured for this interface or area since admin-state was last set to 'enabled'.
Configurable	False

bad-packet-type *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-packet-type <i>number</i>
Tree	bad-packet-type
Description	The total number of OSPF packets received with an invalid OSPF packet type since admin-state was last set to 'enabled'.
Configurable	False

bad-version *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-version <i>number</i>
Tree	bad-version
Description	The total number of OSPF packets received with bad OSPF version numbers since admin-state was last set to 'enabled'.
Configurable	False

bad-virtual-link *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bad-packets bad-virtual-link <i>number</i>
Tree	bad-virtual-link
Description	The total number of OSPF packets received that are destined to a virtual link that does not exist since admin-state was last set to 'enabled'.
Configurable	False

bdr-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> bdr-id <i>string</i>
Tree	bdr-id
Description	the value of BDR-id indicates the router ID of the backup designated router.
Configurable	False

dead-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> dead-interval <i>number</i>
Tree	dead-interval
Description	Time OSPF waits without receiving Hello packets before declaring a neighbor down
Range	2 to 65535
Default	40
Units	seconds
Configurable	True

dr-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> dr-id <i>string</i>
Tree	dr-id
Description	the value of DR-id indicates the router ID of the designated router.
Configurable	False

events *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> events <i>number</i>
Tree	events
Description	the value of events indicates the number of times this OSPF interface has changed its state, or an error has occurred.
Configurable	False

failure-detection

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> failure-detection
Tree	failure-detection
Description	Options related to methods of detecting BGP session failure
Configurable	True

enable-bfd *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Description	Enables the use of BFD for liveliness detection
Default	false
Configurable	True

hello-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> hello-interval <i>number</i>
Tree	hello-interval
Description	Time between OSPF Hellos of this interface
Range	1 to 65535
Default	10
Units	seconds
Configurable	True

interface-type *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> interface-type <i>keyword</i>
Tree	interface-type
Description	Interface type to broadcast or point-to-point
Options	<ul style="list-style-type: none">• broadcast• point-to-point
Configurable	True

last-enabled-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> last-enabled-time <i>string</i>
Tree	last-enabled-time
Description	The value of last-enabled-time indicates the sys-up-time value when ospf-if-admin-stat was last set to enabled (1) to run the ospf on this interface.
Configurable	False

last-event-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> last-event-time <i>string</i>
Tree	last-event-time
Description	The value of last-event-time indicates the value of sys-up-time when an event was last associated with this OSPF interface.
Configurable	False

link-lsa-cksum-sum *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> link-lsa-cksum-sum <i>number</i>
Tree	link-lsa-cksum-sum
Description	the value of link-lsa-cksum-sum indicates the 32-bit unsigned sum of the link-scope link-state advertisements' LS checksums contained in this link's link-state database. the sum can be used to determine if there has been a change in a router's link-state database, and to compare the link state database of two routers.
Configurable	False

link-lsa-count *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> link-lsa-count <i>number</i>
Tree	link-lsa-count
Description	The value of link-lsa-count indicates the total number of link-scope link-state advertisements in this link's link-state database.
Configurable	False

local-ip-address *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> local-ip-address <i>string</i>
Tree	local-ip-address
Description	The value of local-ip-address indicates the IP address of this OSPF interface.
Configurable	False

lsa-filter-out *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> lsa-filter-out <i>keyword</i>
Tree	lsa-filter-out
Description	LSA flooding reduction
Default	none
Options	<ul style="list-style-type: none">• none• all• except-own-rtrlsa• except-own-rtrlsa-and-defaults
Configurable	True

metric *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> metric <i>number</i>
Tree	metric
Description	Explicit route cost metric that is applied to the interface
Configurable	True

mtu *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> mtu <i>number</i>
Tree	mtu
Description	MTU for the OSPF to use on the interface
Range	512 to 9198
Configurable	True

neighbor router-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i>
Tree	neighbor
Description	List of neighbors associated with this OSPF interface
Configurable	False

router-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i>
Description	The router-id advertised by the neighbor
Configurable	False

adjacency-state *identityref*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i> adjacency-state <i>identityref</i>
Tree	adjacency-state
Description	Current OSPF Neighbor state
Options	<ul style="list-style-type: none">• DOWN The initial state of a neighbor, indicating that no recent information has been received from the neighbor.• ATTEMPT Utilised for neighbors that are attached to NBMA networks, it indicates that no information has been recently received from the neighbor but that Hello packets should be directly sent to that neighbor.• INIT Indicates that a Hello packet has been received from the neighbor but bi-directional communication has not yet been established. That is to say that the local Router ID does not appear in the list of neighbors in the remote system's Hello packet.• TWO_WAY Communication between the local and remote system is bi-directional such that the local system's Router ID is listed in the received remote system's Hello packet.• EXSTART An adjacency with the remote system is being formed. The local system is currently transmitting empty database description packets in order to establish the master/slave relationship for the adjacency.• EXCHANGE The local and remote systems are currently exchanging database description packets in order to determine which elements of their local LSDBs are out of date.

- **LOADING**
The local system is sending Link State Request packets to the remote system in order to receive the more recently LSAs that were discovered during the Exchange phase of the procedure establishing the adjacency.
- **FULL**
The neighboring routers are fully adjacent such that both LSDBs are synchronized. The adjacency will appear in Router and Network LSAs

Configurable False

backup-designated-router *string*

Context **network-instance name** *string* **protocols ospfv2 instance name** *string* **area area-id** *string*
interface interface-name *reference* **neighbor router-id** *string* **backup-designated-router**
string

Tree **backup-designated-router**

Description Advertised backup designated router

Configurable False

dead-time *number*

Context **network-instance name** *string* **protocols ospfv2 instance name** *string* **area area-id** *string*
interface interface-name *reference* **neighbor router-id** *string* **dead-time** *number*

Tree **dead-time**

Description The remaining number of seconds remaining in the neighbor's dead time interval

Configurable False

designated-router *string*

Context **network-instance name** *string* **protocols ospfv2 instance name** *string* **area area-id** *string*
interface interface-name *reference* **neighbor router-id** *string* **designated-router** *string*

Tree **designated-router**

Description Advertised designated router

Configurable False

last-established-time *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i> last-established-time <i>number</i>
Tree	last-established-time
Description	Time then OSPF neighbor was last established
Configurable	False

optional-capabilities *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i> optional-capabilities <i>string</i>
Tree	optional-capabilities
Description	Advertised Optional Capabilities
Configurable	False

priority *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i> priority <i>number</i>
Tree	priority
Description	Router priority advertised by neighbor
Configurable	False

retransmission-queue-length *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i> retransmission-queue-length <i>number</i>
Tree	retransmission-queue-length
Description	
Configurable	False

state-changes *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor router-id <i>string</i> state-changes <i>number</i>
Tree	state-changes
Description	total numer of OSPF state changes
Configurable	False

neighbor-count *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> neighbor-count <i>number</i>
Tree	neighbor-count
Description	The total number of OSPF neighbors adjacent on this interface, in a state of INIT or greater, since admin-state was last set to 'enabled'.
Configurable	False

oper-metric *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> oper-metric <i>number</i>
Tree	oper-metric
Description	the value of metric-value indicates the metric value this interface is using. the default value of the metric is (reference bandwidth / if-speed). the value of the reference bandwidth is configured by the reference-bandwidth object.
Range	0 to 65535
Configurable	False

oper-mtu *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> oper-mtu <i>number</i>
Tree	oper-mtu
Description	the value of oper-MTU indicates the operational size of the largest packet which can be sent/received on this OSPF interface, specified in octets. this size DOES include the underlying IP header length, but not the underlying layer headers/trailers.
Configurable	False

oper-state *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
Description	the OSPF interface state.
Options	<ul style="list-style-type: none">• down• loopback• waiting• point-to-point• designated-router• backup-designated-router• other-designated-router
Configurable	False

packets

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets
Tree	packets
Description	Packet counters
Configurable	False

discarded *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets discarded <i>number</i>
Tree	discarded
Description	The total number of OSPF packets discarded since admin-state was last set to 'enabled'.
Configurable	False

retransmits *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets retransmits <i>number</i>
Tree	retransmits
Description	The total number of OSPF retransmits since admin-state was last set to 'enabled'.
Configurable	False

rx-db-description *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets rx-db-description <i>number</i>
Tree	rx-db-description
Description	The total number of OSPF database description packets received since admin-state was last set to 'enabled'.
Configurable	False

rx-hello *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets rx-hello <i>number</i>
Tree	rx-hello
Description	The total number of OSPF hello packets received since admin-state was last set to 'enabled'.
Configurable	False

rx-ls-ack *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets rx-ls-ack <i>number</i>
Tree	rx-ls-ack
Description	The total number of link state acknowledgements received since admin-state was last set to 'enabled'.
Configurable	False

rx-ls-request *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets rx-ls-request <i>number</i>
Tree	rx-ls-request
Description	The total number of link state requests (LS-rs) received since admin-state was last set to 'enabled'.
Configurable	False

rx-ls-update *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets rx-ls-update <i>number</i>
Tree	rx-ls-update
Description	The total number of link state updates (LS-us) received since admin-state was last set to 'enabled'.
Configurable	False

rx-total *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets rx-total <i>number</i>
Tree	rx-total
Description	The total number of OSPF packets received since admin-state was last set to 'enabled'.
Configurable	False

tx-db-description *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets tx-db-description <i>number</i>
Tree	tx-db-description
Description	The total number of OSPF database description packets transmitted since admin-state was last set to 'enabled'.
Configurable	False

tx-hello *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets tx-hello <i>number</i>
Tree	tx-hello
Description	The total number of OSPF hello packets transmitted since admin-state was last set to 'enabled'.
Configurable	False

tx-ls-ack *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets tx-ls-ack <i>number</i>
Tree	tx-ls-ack
Description	The total number of OSPF link state acknowledgements transmitted since admin-state was last set to 'enabled'.
Configurable	False

tx-ls-request *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets tx-ls-request <i>number</i>
Tree	tx-ls-request
Description	The total number of OSPF link state requests (LS-rs) transmitted since admin-state was last set to 'enabled'.
Configurable	False

tx-ls-update *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets tx-ls-update <i>number</i>
Tree	tx-ls-update
Description	The total number of OSPF link state updates (LS-us) transmitted since admin-state was last set to 'enabled'.
Configurable	False

tx-total *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> packets tx-total <i>number</i>
Tree	tx-total
Description	The total number of OSPF packets transmitted since admin-state was last set to 'enabled'.
Configurable	False

passive *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> passive <i>boolean</i>
Tree	passive
Description	Allow interface to be advertised as an OSPF interface without running the OSPF protocol
Configurable	True

priority *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> priority <i>number</i>
Tree	priority
Description	Priority of the interface to apply in the designated router election on the subnet
Range	0 to 255
Default	1
Configurable	True

retransmit-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> retransmit-interval <i>number</i>
Tree	retransmit-interval
Description	Time before OSPF retransmits an unacknowledged LSA to a neighbor
Range	1 to 1800
Default	5
Units	seconds
Configurable	True

transit-delay *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> transit-delay <i>number</i>
Tree	transit-delay
Description	Time required to transmit an LSA on the interface, virtual link, or sham link
Range	1 to 1800
Default	1
Units	seconds
Configurable	True

type *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> interface interface-name <i>reference</i> type <i>keyword</i>
Tree	type
Description	The value of type indicates the operational OSPF interface type.
Options	<ul style="list-style-type: none">• broadcast• point-to-point
Configurable	False

nssa

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa
Tree	nssa
Description	This command creates the context to configure the associated OSPF or OSPF3 area as Not So Stubby Area (NSSA). NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF or OSPF3 domain.
Configurable	True

area-range ip-prefix-mask *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa area-range ip-prefix-mask <i>string</i>
Tree	area-range
Description	Enter the area-range context
Configurable	True

ip-prefix-mask *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa area-range ip-prefix-mask <i>string</i>
Description	ip-prefix a.b.c.d (host bits must be 0) mask [0..32]
Configurable	True

advertise *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa area-range ip-prefix-mask <i>string</i> advertise <i>boolean</i>
Tree	advertise
Description	Advertise summarized range of addresses to other areas
Default	true
Configurable	True

originate-default-route

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa originate-default-route
Tree	originate-default-route
Description	Enter the originate-default-route context
Configurable	True

adjacency-check *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa originate-default-route adjacency-check <i>boolean</i>
Tree	adjacency-check
Description	Default route to remove if there is no adjacency
Default	true
Configurable	True

type-nssa *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa originate-default-route type-nssa <i>boolean</i>
Tree	type-nssa
Description	Generate a default route using NSSA-LSA type
Default	false
Configurable	True

redistribute-external *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa redistribute-external <i>boolean</i>
Tree	redistribute-external
Description	Enables the redistribution of external routes into the Not So Stubby Area (NSSA) or an NSSA area border router (ABR) that is exporting the routes into non-NSSA areas
Configurable	True

summaries *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> nssa summaries <i>boolean</i>
Tree	summaries
Description	Enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR)
Configurable	True

stub

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> stub
Tree	stub
Description	
Configurable	True

default-metric *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> stub default-metric <i>number</i>
Tree	default-metric
Description	Defines the default OSPF metric for associated stub area
Configurable	True

summaries *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area area-id <i>string</i> stub summaries <i>boolean</i>
Tree	summaries
Description	Enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR)
Configurable	True

area-border-router *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> area-border-router <i>boolean</i>
Tree	area-border-router
Description	This indicates whether this router is an area border router.
Configurable	False

as-border-router *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> as-border-router <i>boolean</i>
Tree	as-border-router
Description	This indicates whether this router is an AS border router.
Configurable	False

asbr

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> asbr
Tree	asbr
Description	Configure the router as an ASBR (Autonomous System Boundary Router)
Configurable	True

trace-path (*number | keyword*)

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> asbr trace-path (<i>number keyword</i>)
Tree	trace-path
Description	Domain identity
Range	0 to 31
Default	none
Options	<ul style="list-style-type: none">• none
Configurable	True

backbone-router *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> backbone-router <i>boolean</i>
Tree	backbone-router
Description	This indicates whether or not this router is configured as an OSPF back bone router.
Configurable	False

export-limit

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> export-limit
Tree	export-limit
Description	Enter the export-limit context
Configurable	True

log-percent *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> export-limit log-percent <i>number</i>
Tree	log-percent
Description	Export limit at which warning a log message and SNMP notification are sent
Range	1 to 100
Configurable	True

number *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> export-limit number <i>number</i>
Tree	number
Description	Maximum number of routes or prefixes to be exported into IGP instance from route table
Range	1 to max
Configurable	True

export-policy *reference*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> export-policy <i>reference</i>
Tree	export-policy
Description	Apply an export policy to redistribute non-OSPFv2 routes into OSPF
Reference	routing-policy policy name <i>string</i>
Configurable	True

external-db-overflow

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> external-db-overflow
Tree	external-db-overflow
Description	
Configurable	True

interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> external-db-overflow interval <i>number</i>
Tree	interval
Description	Set interval value
Range	0 to 2147483647
Default	0
Units	seconds
Configurable	True

limit *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> external-db-overflow limit <i>number</i>
Tree	limit
Description	Set limit value
Range	0 to 2147483647
Default	0
Configurable	True

external-preference *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> external-preference <i>number</i>
Tree	external-preference
Description	Configure the route preference associated with OSPF external routes
Default	150
Configurable	True

graceful-restart

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> graceful-restart
Tree	graceful-restart
Description	Container for options related to OSPFv2 graceful restart
Configurable	True

helper-mode *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> graceful-restart helper-mode <i>boolean</i>
Tree	helper-mode
Description	Enable or disable the IS-IS graceful restart helper function When this leaf is set, the local system supports retaining forwarding information during a neighbor router's restart.
Default	false
Configurable	True

strict-lsa-checking *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> graceful-restart strict-lsa-checking <i>boolean</i>
Tree	strict-lsa-checking
Description	
Default	false
Configurable	True

last-disabled-reason *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-disabled-reason <i>string</i>
Tree	last-disabled-reason
Description	Reason why the disabled state was entered the last time.
String Length	0 to 20
Configurable	False

last-enabled-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-enabled-time <i>string</i>
Tree	last-enabled-time
Description	the value of last-enabled-time indicates the value of sys-up-time when admin-state was last set to 'enabled'. when admin-state is set to 'disabled', the OSPF counters are stopped when admin-state is reset to 'enabled', the counters are reset to zero.
Configurable	False

last-overflow-entered-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-overflow-entered-time <i>string</i>
Tree	last-overflow-entered-time
Description	The value of last-ovrflw-entered-time indicates the value of sys-up-time the last time we entered overflow state. this overflow state occurs when the number of non-default AS-external-LS-as entries exceed the link-state database capability.
Configurable	False

last-overflow-exit-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-overflow-exit-time <i>string</i>
Tree	last-overflow-exit-time
Description	the value of last-overflow-exit-time indicates the value of sys-up-time the last time we exited overflow state. this overflow state occurs when the number of non-default AS-external-LS-as entries exceed the link-state database capability.
Configurable	False

last-overload-enter-code *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-overload-enter-code <i>keyword</i>
Tree	last-overload-enter-code
Description	the value of last-overload-enter-code indicates the condition which caused OSPF to get into overload.
Options	<ul style="list-style-type: none">• none• spf-failed• boot-overload• manual-overload• sfm-overload• fib-add-fail• rtm-add-fail• rtr-adv-lsa-limit
Configurable	False

last-overload-entered-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-overload-entered-time <i>string</i>
Tree	last-overload-entered-time
Description	the value of last-overload-entrd-time indicates the time at which the system last went into overload state.
Configurable	False

last-overload-exit-code *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-overload-exit-code <i>keyword</i>
Tree	last-overload-exit-code
Description	the value of last-overload-exit-code indicates the reason why OSPF came out of overload state the last time, since reset.
Options	<ul style="list-style-type: none">• none• bgp-sig-recv• timer-expired• manual-exit• sfm-overload-done
Configurable	False

last-overload-exit-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> last-overload-exit-time <i>string</i>
Tree	last-overload-exit-time
Description	the value of last-overload-exit-time indicates the time at which the system last came out of overload state.
Configurable	False

log-adjacency-changes *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> log-adjacency-changes <i>boolean</i>
Tree	log-adjacency-changes
Description	
Configurable	True

max-ecmp-paths *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> max-ecmp-paths <i>number</i>
Tree	max-ecmp-paths
Description	The maximum number of ECMP next-hops to program into the FIB for every IP prefix
Range	1 to 64
Default	1
Configurable	True

oper-router-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> oper-router-id <i>string</i>
Tree	oper-router-id
Description	the value of oper-router-id indicates the 32-bit integer used to uniquely identify the router in the autonomous system. the default OSPF instance will use the value specified by router-id or the one derived from the IP layer. For the non-default instances of OSPF, this is the same value as router-id, which must be specified before the OSPF instance can become operational.
Configurable	False

oper-state *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Description	Used to report operational state of the OSPF instance
Options	<ul style="list-style-type: none">• enable• disable
Configurable	False

overflow *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overflow <i>boolean</i>
Tree	overflow
Description	The value of in-overflow-state indicates the current overflow state (true/false). This overflow state occurs when the number of non-default AS-external-LS-as entries exceed the link-state database capability.
Configurable	False

overload

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload
Tree	overload
Description	
Configurable	True

active *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload active <i>boolean</i>
Tree	active
Description	Set to active
Default	false
Configurable	True

overload-include-ext-1 *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload overload-include-ext-1 <i>boolean</i>
Tree	overload-include-ext-1
Description	
Default	false
Configurable	True

overload-include-ext-2 *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload overload-include-ext-2 <i>boolean</i>
Tree	overload-include-ext-2
Description	
Default	false
Configurable	True

overload-include-ext-stub *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload-include-ext-stub <i>boolean</i>
Tree	overload-include-ext-stub
Description	
Default	false
Configurable	True

overload-on-boot

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload-on-boot
Tree	overload-on-boot
Description	
Configurable	True

timeout *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload-on-boot timeout <i>number</i>
Tree	timeout
Description	Specifies the time that the router should remain in overload state after the OSPF process restarts
Range	1 to 1800
Default	60
Units	seconds
Configurable	True

rtr-adv-lsa-limit

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> rtr-adv-lsa-limit
Tree	rtr-adv-lsa-limit
Description	
Configurable	True

log-only *boolean*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload rtr-adv-lsa-limit log-only <i>boolean</i>
Tree	log-only
Description	
Configurable	True

max-lsa-count *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload rtr-adv-lsa-limit max-lsa-count <i>number</i>
Tree	max-lsa-count
Description	
Range	1 to 4294967295
Configurable	True

overload-timeout *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload rtr-adv-lsa-limit overload-timeout <i>number</i>
Tree	overload-timeout
Description	
Range	1 to 1800
Configurable	True

warning-threshold *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload rtr-adv-lsa-limit warning-threshold <i>number</i>
Tree	warning-threshold
Description	
Range	0 to 100
Default	0
Configurable	True

overload-rem-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload-rem-interval <i>number</i>
Tree	overload-rem-interval
Description	the value of overload-rem-interval indicates the time for which the system will be in overload state if OSPF is in overload state. the value of 0 implies that the system is indefinitely in overload state.
Range	0 to 65535
Units	seconds
Configurable	False

overload-state *keyword*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> overload-state <i>keyword</i>
Tree	overload-state
Description	the value of overload-oper-state indicates whether or not the OSPF application is presently in overload state or not.
Options	<ul style="list-style-type: none">• overload• no-overload
Configurable	False

ovld-lsa-limit-rem-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> ovld-lsa-limit-rem-interval <i>number</i>
Tree	ovld-lsa-limit-rem-interval
Description	the value of ovld-lsa-limit-rem-interval indicates the remaining time in seconds for which the system will be in overload state due to advertising router LSA limit exceeded. the value of 0 implies that the system is either not in overload or indefinitely in overload state.
Range	0 to 65535
Units	seconds
Configurable	False

preference *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> preference <i>number</i>
Tree	preference
Description	Sets the route preference for OSPF sourced routes
Range	1 to 255
Default	10
Configurable	True

reference-bandwidth *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> reference-bandwidth <i>number</i>
Tree	reference-bandwidth
Description	<p>Configures the reference bandwidth that provides the basis for interface metrics based on link Bandwidth</p> <p>If the reference bandwidth is defined, then the cost is calculated using the following formula: cost = reference-bandwidth / bandwidth</p> <p>When a large reference-bandwidth value is configured, a metric calculation may result in a value higher than the supported protocol cost value. If this occurs, OSPFv2 automatically reverts to the maximum configurable cost metric.</p> <p>If the reference bandwidth is not configured then all interfaces have a default metric of 10.</p> <p>Note: To use metrics in excess of 63, wide metrics must be deployed</p>
Range	1 to 100000000
Units	kbps
Configurable	True

router-id *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> router-id <i>string</i>
Tree	router-id
Description	
Configurable	True

routes-submitted *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> routes-submitted <i>number</i>
Tree	routes-submitted
Description	the value of routes-submitted indicates the number of routes submitted to the route table manager (RTM) by this instance of OSPF.
Configurable	False

spf

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf
Tree	spf
Description	SPF related information
Configurable	False

avg-spf-run-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> avg-spf-run-interval <i>number</i>
Tree	avg-spf-run-interval
Description	the value of avg-spf-run-interval indicates the average time, in hundredths of seconds, of all the total SPF calculations performed by this OSPF router.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

ext-spf-runs *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf ext-spf-runs <i>number</i>
Tree	ext-spf-runs
Description	The total number of times that only the external portion of the SPF has been run since OSPF was last enabled.
Configurable	False

full-spf-runs *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf full-spf-runs <i>number</i>
Tree	full-spf-runs
Description	The total number of times that complete SPF has been run on the router since OSPF was last enabled.
Configurable	False

incremental-ext-spf-runs *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf incremental-ext-spf-runs <i>number</i>
Tree	incremental-ext-spf-runs
Description	The total number of incremental SPF runs triggered by new or updated external LS-as.
Configurable	False

incremental-inter-spf-runs *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf incremental-inter-spf-runs <i>number</i>
Tree	incremental-inter-spf-runs
Description	The total number of incremental SPF runs triggered by new or updated inter-area prefix or inter-area router LS-as.
Configurable	False

last-ext-spf

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-ext-spf
Tree	last-ext-spf
Description	Information about the last external SPF run
Configurable	False

interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-ext-spf interval <i>number</i>
Tree	interval
Description	the value of ext-spf-run-interval indicates the time, in hundredths of seconds, used to perform the most recent total external (not incremental) SPF calculation.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

run-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-ext-spf run-time <i>string</i>
Tree	run-time
Description	the value of last-ext-spf-run-time indicates the value of sys-up-time when the external OSPF dijkstra (SPF) was last run.
Configurable	False

last-full-spf

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf
Tree	last-full-spf
Description	Information about the last full SPF run
Configurable	False

extern-spf-time *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf extern-spf-time <i>number</i>
Tree	extern-spf-time
Description	Time it took, in hundredths of seconds, to complete the external LSA calculations.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

inter-spf-time *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf inter-spf-time <i>number</i>
Tree	inter-spf-time
Description	Time it took, in hundredths of seconds, to complete the inter-area SPF calculations.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

intra-spf-time *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf intra-spf-time <i>number</i>
Tree	intra-spf-time
Description	Time it took, in hundredths of seconds, to complete the intra-area SPF calculations.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

rtm-update-time *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf rtm-update-time <i>number</i>
Tree	rtm-update-time
Description	Time it took, in hundredths of seconds, to complete the RTM updates.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

run-time *string*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf run-time <i>string</i>
Tree	run-time
Description	the value of last-full-spf-run-time indicates the time at which the system last performed a full dijkstra (SPF) run.
Configurable	False

total-time *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf last-full-spf total-time <i>number</i>
Tree	total-time
Description	Time it took, in hundredths of seconds, to complete the last SPF run completely.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

max-spf-run-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf max-spf-run-interval <i>number</i>
Tree	max-spf-run-interval
Description	the value of max-spf-run-interval indicates the maximum time, in hundredths of seconds, used to perform a total SPF calculation.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

min-spf-run-interval *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf min-spf-run-interval <i>number</i>
Tree	min-spf-run-interval
Description	the value of min-spf-run-interval indicates the minimum time, in hundredths of seconds, used to perform a total SPF calculation.
Range	0 to 2147483647
Units	centiseconds
Configurable	False

spf-attempts-failed *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> spf spf-attempts-failed <i>number</i>
Tree	spf-attempts-failed
Description	The number of times an attempt to run SPF has failed because SPF runs have been stopped as a result of insufficient memory resources.
Configurable	False

timers

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers
Tree	timers
Description	Enter the timers context
Configurable	True

incremental-spf-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers incremental-spf-wait <i>number</i>
Tree	incremental-spf-wait
Description	Delay time before an incremental SPF calculation is started
Range	0 to 1000
Default	1000
Configurable	True

lsa-accumulate *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers lsa-accumulate <i>number</i>
Tree	lsa-accumulate
Description	Delay time for accumulating multiple LSAs before advertising them to neighbors
Range	0 to 1000
Default	1000
Configurable	True

Isa-arrival *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers Isa-arrival number
Tree	Isa-arrival
Description	Minimum delay between receipt of the same LSAs arriving from neighbors
Range	0 to 600000
Default	1000
Configurable	True

Isa-generate

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers Isa-generate
Tree	Isa-generate
Description	Enter the Isa-generate context
Configurable	True

Isa-initial-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers Isa-generate Isa-initial-wait number
Tree	Isa-initial-wait
Description	First waiting period between link state advertisements LSA originates
Range	10 to 600000
Default	5000
Units	milliseconds
Configurable	True

lsa-second-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers lsa-generate lsa-second-wait <i>number</i>
Tree	lsa-second-wait
Description	Hold time between the first and second LSA generation
Range	10 to 600000
Default	5000
Units	milliseconds
Configurable	True

max-lsa-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers lsa-generate max-lsa-wait <i>number</i>
Tree	max-lsa-wait
Description	Maximum time between two consecutive occurrences of an LSA being generated
Range	10 to 600000
Default	5000
Units	milliseconds
Configurable	True

redistribute-delay *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers redistribute-delay <i>number</i>
Tree	redistribute-delay
Description	Hold down timer for external routes that are redistributed in OSPF
Range	0 to 1000
Default	1000
Configurable	True

spf-wait

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers spf-wait
Tree	spf-wait
Description	Enter the spf-wait context
Configurable	True

spf-initial-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers spf-wait spf-initial-wait <i>number</i>
Tree	spf-initial-wait
Description	Initial SPF calculation delay after a topology change
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

spf-max-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers spf-wait spf-max-wait <i>number</i>
Tree	spf-max-wait
Description	Maximum interval between two consecutive SPF calculations
Range	10 to 120000
Default	10000
Units	milliseconds
Configurable	True

spf-second-wait *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> timers spf-wait spf-second-wait <i>number</i>
Tree	spf-second-wait
Description	Hold time between the first and second SPF calculation
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

total-exported-routes *number*

Context	network-instance name <i>string</i> protocols ospfv2 instance name <i>string</i> total-exported-routes <i>number</i>
Tree	total-exported-routes
Description	the value of total-exported-routes indicates the total number of routes exported into OSPF from the route table manager when an export policy is configured. value of total-exported-routes would be 0 when no export policy is configured.
Configurable	False

route-table

Context	network-instance name <i>string</i> route-table
Tree	route-table
Description	
Configurable	False

ipv4-unicast

Context	network-instance name <i>string</i> route-table ipv4-unicast
Tree	ipv4-unicast
Description	The container for the IPv4 unicast routing table of the network instance.
Configurable	False

route ipv4-prefix *string id number*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string id number</i>
Tree	route
Description	
Configurable	False

ipv4-prefix *string*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string id number</i>
Description	
Configurable	False

id *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i>
Description	An index value representing the relative order of preference of routes for the same prefix. If there is an active route for the prefix it will always be assigned index 0. The route with index 1 is next in order to become active if the route with index 0 is removed.
Configurable	False

active *boolean*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> active <i>boolean</i>
Tree	active
Description	If set to true then the route is installed as the active route for the IP prefix in the FIB. A route can be inactive because there is a more preferred route for the same prefix or else its next-hops are unresolved.
Configurable	False

fib-programming

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> fib-programming
Tree	fib-programming
Description	Container for state related to the FIB programming of the route
Configurable	False

failed-slots *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> fib-programming failed-slots <i>number</i>
Tree	failed-slots
Description	The list of slot IDs corresponding to the linecards that did not successfully program the route due to the FIB table being full
Range	1 to 8
Configurable	False

status *keyword*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> fib-programming status <i>keyword</i>
Tree	status
Description	The status of the FIB programming
Options	<ul style="list-style-type: none">• success The route was downloaded to the linecards and all of them have sent an acknowledgement that covers the route.• failed The route was not programmed into the FIB table of one or more linecards due to the FIB table being full.• pending The route was downloaded to the linecards but some of them have not sent an acknowledgement yet.
Configurable	False

last-app-update *string*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> last-app-update <i>string</i>
Tree	last-app-update
Description	The date and time of the last update of this route by the owning application or protocol.
Configurable	False

metric *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> metric <i>number</i>
Tree	metric
Description	The metric of the IP route. In general, when comparing two routes with the same owner and preference, the route with the lower metric is the one that is activated and used for forwarding.
Configurable	False

next-hop-group *reference*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> next-hop-group <i>reference</i>
Tree	next-hop-group
Description	The next-hop-group indirection object used by this route.
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False

owner *identityref*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> owner <i>identityref</i>
Tree	owner
Description	The protocol or application that owns the IP route
Options	<ul style="list-style-type: none">• bgp Border Gateway Protocol version 4• isis IS-IS• ospfv2 OSPFv2• ospfv3 OSPFv3• static Locally configured static route• local A directly connected route• host A host route• aggregate Locally configured aggregate route• sdk IP route added by an agent application using the SDK• linux-mgr IP route added by the linux kernel.• dhcp-client-mgr IP route added by DHCP client
Configurable	False

preference *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> preference <i>number</i>
Tree	preference
Description	The IP route table preference. This is sometimes called the administrative distance of the route. In general, when comparing any two routes, the route with the lower preference is the one that is activated and used for forwarding.
Configurable	False

resilient-hash *boolean*

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> id <i>number</i> resilient-hash <i>boolean</i>
Tree	resilient-hash
Description	Set to true if the route is covered by a resilient-hash-prefix entry
Configurable	False

statistics

Context	network-instance name <i>string</i> route-table ipv4-unicast statistics
Tree	statistics
Description	Display statistics
Configurable	False

active-entries *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast statistics active-entries <i>number</i>
Tree	active-entries
Description	The total number of entries that are active in the FIB.
Default	0
Configurable	False

active-entries-with-ecmp *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast statistics active-entries-with-ecmp <i>number</i>
Tree	active-entries-with-ecmp
Description	The total number of entries that are active in the FIB and that have multiple ECMP next-hops.
Default	0
Configurable	False

total-entries *number*

Context	network-instance name <i>string</i> route-table ipv4-unicast statistics total-entries <i>number</i>
Tree	total-entries
Description	The total number of routes, active and inactive, belonging to this address family, that are present in the routing table.
Default	0
Configurable	False

ipv6-unicast

Context	network-instance name <i>string</i> route-table ipv6-unicast
Tree	ipv6-unicast
Description	The container for the IPv6 unicast routing table of the network instance.
Configurable	False

route ipv6-prefix *string id number*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string id number</i>
Tree	route
Description	
Configurable	False

ipv6-prefix *string*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string id number</i>
Description	
Configurable	False

id *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i>
Description	An index value representing the relative order of preference of routes for the same prefix. If there is an active route for the prefix it will always be assigned index 0. The route with index 1 is next in order to become active if the route with index 0 is removed.
Configurable	False

active *boolean*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> active <i>boolean</i>
Tree	active
Description	If set to true then the route is installed as the active route for the IP prefix in the FIB. A route can be inactive because there is a more preferred route for the same prefix or else its next-hops are unresolved.
Configurable	False

fib-programming

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> fib-programming
Tree	fib-programming
Description	Container for state related to the FIB programming of the route
Configurable	False

failed-slots *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> fib-programming failed-slots <i>number</i>
Tree	failed-slots
Description	The list of slot IDs corresponding to the linecards that did not successfully program the route due to the FIB table being full
Range	1 to 8
Configurable	False

status *keyword*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> fib-programming status <i>keyword</i>
Tree	status
Description	The status of the FIB programming
Options	<ul style="list-style-type: none">• success The route was downloaded to the linecards and all of them have sent an acknowledgement that covers the route.• failed The route was not programmed into the FIB table of one or more linecards due to the FIB table being full.• pending The route was downloaded to the linecards but some of them have not sent an acknowledgement yet.
Configurable	False

last-app-update *string*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> last-app-update <i>string</i>
Tree	last-app-update
Description	The date and time of the last update of this route by the owning application or protocol.
Configurable	False

metric *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> metric <i>number</i>
Tree	metric
Description	The metric of the IP route. In general, when comparing two routes with the same owner and preference, the route with the lower metric is the one that is activated and used for forwarding.
Configurable	False

next-hop-group *reference*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> next-hop-group <i>reference</i>
Tree	next-hop-group
Description	The next-hop-group indirection object used by this route.
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False

owner *identityref*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> owner <i>identityref</i>
Tree	owner
Description	The protocol or application that owns the IP route
Options	<ul style="list-style-type: none">• bgp Border Gateway Protocol version 4• isis IS-IS• ospfv2 OSPFv2• ospfv3 OSPFv3• static Locally configured static route• local A directly connected route• host A host route• aggregate Locally configured aggregate route• sdk IP route added by an agent application using the SDK• linux-mgr IP route added by the linux kernel.• dhcp-client-mgr IP route added by DHCP client
Configurable	False

preference *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> preference <i>number</i>
Tree	preference
Description	The IP route table preference. This is sometimes called the administrative distance of the route. In general, when comparing any two routes, the route with the lower preference is the one that is activated and used for forwarding.
Configurable	False

resilient-hash *boolean*

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> id <i>number</i> resilient-hash <i>boolean</i>
Tree	resilient-hash
Description	Set to true if the route is covered by a resilient-hash-prefix entry
Configurable	False

statistics

Context	network-instance name <i>string</i> route-table ipv6-unicast statistics
Tree	statistics
Description	Display statistics
Configurable	False

active-entries *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast statistics active-entries <i>number</i>
Tree	active-entries
Description	The total number of entries that are active in the FIB.
Default	0
Configurable	False

active-entries-with-ecmp *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast statistics active-entries-with-ecmp <i>number</i>
Tree	active-entries-with-ecmp
Description	The total number of entries that are active in the FIB and that have multiple ECMP next-hops.
Default	0
Configurable	False

total-entries *number*

Context	network-instance name <i>string</i> route-table ipv6-unicast statistics total-entries <i>number</i>
Tree	total-entries
Description	The total number of routes, active and inactive, belonging to this address family, that are present in the routing table.
Default	0
Configurable	False

mpls

Context	network-instance name <i>string</i> route-table mpls
Tree	mpls
Description	The container for the MPLS routing table of the network instance.
Configurable	False

route label (*number | keyword*) **id** *number*

Context	network-instance name <i>string</i> route-table mpls route label (<i>number keyword</i>) id <i>number</i>
Tree	route
Description	
Configurable	False

label (*number | keyword*)

Context	network-instance name <i>string</i> route-table mpls route label (<i>number keyword</i>) id <i>number</i>
Description	
Range	16 to 1048575
Options	<ul style="list-style-type: none">• IMPLICIT_NULL

assigned by local LSR but not carried in packets

Configurable False

id number

Context **network-instance name** *string* **route-table mpls route label** (*number | keyword*) **id** *number*

Description An index value representing the relative order of preference of entries for the same label. If there is an active entry for the label it will always be assigned index 0. The entry with index 1 is next in order to become active if the entry with index 0 is removed.

Configurable False

active boolean

Context **network-instance name** *string* **route-table mpls route label** (*number | keyword*) **id** *number*
active *boolean*

Tree **active**

Description If set to true then the route is installed as the active entry for the label value in the FIB. A route can be inactive because there is a more preferred route for the same label value or else its next-hops are unresolved.

Configurable False

fib-change-pending boolean

Context **network-instance name** *string* **route-table mpls route label** (*number | keyword*) **id** *number*
fib-change-pending *boolean*

Tree **fib-change-pending**

Description If set to true then a create, delete or update of the route by its owner application has occurred recently but not all linecards have acknowledged the change yet.

Configurable False

last-app-update string

Context **network-instance name** *string* **route-table mpls route label** (*number | keyword*) **id** *number*
last-app-update *string*

Tree **last-app-update**

Description The date and time of the last update of this route by the owning application or protocol.

Configurable False

next-hop-group *reference*

Context	network-instance name <i>string</i> route-table mpls route label (<i>number keyword</i>) id <i>number</i> next-hop-group <i>reference</i>
Tree	next-hop-group
Description	The next-hop-group indirection object used by this route.
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False

owner *identityref*

Context	network-instance name <i>string</i> route-table mpls route label (<i>number keyword</i>) id <i>number</i> owner <i>identityref</i>
Tree	owner
Description	The protocol or application that owns the MPLS label entry.
Options	<ul style="list-style-type: none">• mpls-static Locally configured static route• mpls-sdk MPLS label entry added by an agent application using the SDK
Configurable	False

preference *number*

Context	network-instance name <i>string</i> route-table mpls route label (<i>number keyword</i>) id <i>number</i> preference <i>number</i>
Tree	preference
Description	The MPLS route table preference. This is sometimes called the administrative distance of the route. In general, when comparing any two entries, the route with the lower preference is the one that is activated and used for forwarding.
Configurable	False

statistics

Context	network-instance name <i>string</i> route-table mpls statistics
Tree	statistics
Description	Display statistics
Configurable	False

active-entries *number*

Context	network-instance name <i>string</i> route-table mpls statistics active-entries <i>number</i>
Tree	active-entries
Description	The total number of MPLS entries that are active in the FIB.
Default	0
Configurable	False

active-entries-with-ecmp *number*

Context	network-instance name <i>string</i> route-table mpls statistics active-entries-with-ecmp <i>number</i>
Tree	active-entries-with-ecmp
Description	The total number of MPLS entries that are active in the FIB and that have multiple ECMP next-hops.
Default	0
Configurable	False

total-entries *number*

Context	network-instance name <i>string</i> route-table mpls statistics total-entries <i>number</i>
Tree	total-entries
Description	The total number of MPLS entries that are present in the routing table.
Default	0
Configurable	False

next-hop index *number*

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i>
Tree	next-hop
Description	
Configurable	False

index *number*

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i>
Description	A system-wide unique identifier of a next-hop object (system allocated).
Configurable	False

encapsulate-header *keyword*

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> encapsulate-header <i>keyword</i>
Tree	encapsulate-header
Description	The type of tunneling encapsulation that is applied to packets forwarded to this next-hop.
Options	<ul style="list-style-type: none">• gre• ipv4• ipv6• mpls
Configurable	False

ip-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> ip-address (<i>ipv4-address ipv6-address</i>)
Tree	ip-address
Description	The next-hop IP address. Only populated when the next-hop type is indirect or tunnel.
Configurable	False

pushed-mpls-label-stack (*number | keyword*)

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> pushed-mpls-label-stack (<i>number keyword</i>)
Tree	pushed-mpls-label-stack
Description	The list of MPLS labels to push onto the packet when forwarding to this particular next-hop.
Range	16 to 1048575
Options	<ul style="list-style-type: none">• IMPLICIT_NULL assigned by local LSR but not carried in packets
Configurable	False
Max. Elements	1

resolving-route

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route
Tree	resolving-route
Description	
Configurable	False

ip-prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route ip-prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	ip-prefix
Description	The prefix of the resolving route.
Configurable	False

owner identityref

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route owner <i>identityref</i>
Tree	owner
Description	The owner of the resolving route.
Options	<ul style="list-style-type: none">• bgp Border Gateway Protocol version 4• isis IS-IS• ospfv2 OSPFv2• ospfv3 OSPFv3• static Locally configured static route• local A directly connected route• host A host route• aggregate Locally configured aggregate route• sdk IP route added by an agent application using the SDK• linux-mgr IP route added by the linux kernel.• dhcp-client-mgr IP route added by DHCP client
Configurable	False

subinterface *reference*

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> subinterface <i>reference</i>
Tree	subinterface
Description	The next-hop interface. Only populated when the next-hop type is direct.
Reference	interface name <i>string</i> subinterface index <i>number</i> name <i>string</i>
Configurable	False

type *identityref*

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> type <i>identityref</i>
Tree	type
Description	The next-hop type used by the datapath.
Options	<ul style="list-style-type: none">• extract Next-hop will cause matching packets to be delivered to the CPM.• direct Next-hop was resolved by a local route - i.e. it is an address on a connected subnet.• discard Next-hop will cause matching packets to be dropped without ICMP generation.• reject Next-hop will cause matching packets to be dropped with ICMP generation.• indirect Next-hop was resolved by a non-local route - i.e. it is not an address on a connected subnet.• tunnel Next-hop was resolved by a tunnel.
Configurable	False

next-hop-group **index** *number*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Tree	next-hop-group
Description	
Configurable	False

index number

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Description	A system-wide unique identifier of a next-hop-group indirection object (system allocated).
Configurable	False

last-app-update *string*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> last-app-update <i>string</i>
Tree	last-app-update
Description	The date and time of the last update of this next-hop-group by the owning application or protocol.
Configurable	False

next-hop id *number*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> next-hop id <i>number</i>
Tree	next-hop
Description	
Configurable	False

id *number*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> next-hop id <i>number</i>
Description	A unique identifier of a next-hop member (system allocated).
Range	0 to 1023
Configurable	False

active *boolean*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> next-hop id <i>number</i> active <i>boolean</i>
Tree	active
Description	If set to true then the next-hop is active and used in the group. It can be inactive if it is not resolved
Configurable	False

next-hop *reference*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> next-hop id <i>number</i> next-hop <i>reference</i>
Tree	next-hop
Description	
Reference	network-instance name <i>string</i> route-table next-hop index <i>number</i>
Configurable	False

owner *identityref*

Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> owner <i>identityref</i>
Tree	owner
Description	The protocol or application that owns the next-hop-group programming.
Options	<ul style="list-style-type: none">• nhg-static Locally configured static next-hop-group• nhg-sdk Next-hop-group added by an agent application using the SDK
Configurable	False

router-id *string*

Context	network-instance name <i>string</i> router-id <i>string</i>
Tree	router-id
Description	A identifier for the local network instance - typically used within associated routing protocols or signalling routing information in another network instance
Configurable	True

static-routes

Context	network-instance name <i>string</i> static-routes
Tree	static-routes
Description	
Configurable	True

route prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	route
Description	
Configurable	True
Max. Elements	16384

prefix (*ipv4-prefix | ipv6-prefix*)

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>)
Description	IPv4 or IPv6 prefix.
Configurable	True

admin-state *keyword*

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) admin-state <i>keyword</i>
Tree	admin-state
Description	Used to disable the static route.
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

installed *boolean*

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) installed <i>boolean</i>
Tree	installed
Description	If set to true, this indicates that the static route was installed into the datapath. If this is false then there are 3 possible reasons: (a) the admin-state is disable (b) there is another IP route for the same prefix that has a superior preference (c) the next-hop-group has no resolvable next-hops
Configurable	False

metric *number*

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) metric number
Tree	metric
Description	IGP metric of the static route.
Default	1
Configurable	True

next-hop-group *reference*

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) next-hop-group reference
Tree	next-hop-group
Description	
Reference	network-instance name <i>string</i> next-hop-groups group name <i>string</i>
Configurable	True

preference *number*

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) preference number
Tree	preference
Description	Route preference with lower values indicating a higher degree of preference.
Range	0 to 255
Default	5
Configurable	True

tcp

Context	network-instance name <i>string</i> tcp
Tree	tcp
Description	State for TCP connections that have been established or could be established using the route tables of this network instance.
Configurable	False

connection **local-address** (*ipv4-address | ipv6-address*) **local-port** *number* **remote-address** (*ipv4-address | ipv6-address*) **remote-port** *number*

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i>
Tree	connection
Description	List of TCP connections that are established or that are in the process of being established – i.e. excluding those in the LISTEN state. An entry in this list is transient in that it ceases to exist when (or soon after) the connection makes the transition to the CLOSED state.
Configurable	False

local-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i>
Description	The local IP address for this TCP connection.
Configurable	False

local-port *number*

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i>
Description	The local port number for this TCP connection.
Range	0 to 65535
Configurable	False

remote-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i>
Description	The remote IP address for this TCP connection.
Configurable	False

remote-port *number*

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i>
Description	The remote port number for this TCP connection.
Range	0 to 65535
Configurable	False

process-id *number*

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i> process-id <i>number</i>
Tree	process-id
Description	The process ID of the application that owns the socket.
Configurable	False

session-state *keyword*

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address ipv6-address</i>) remote-port <i>number</i> session-state <i>keyword</i>
Tree	session-state
Description	The state of this TCP connection.
Options	<ul style="list-style-type: none">• closed• syn-sent• syn-received• established• fin-wait1• fin-wait2• close-wait• last-ack• closing• time-wait• delete-tcb
Configurable	False

listening-application **local-address** (*ipv4-address | ipv6-address*) **local-port** *number*

Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i>
Tree	listening-application
Description	List of applications that are listening on a particular TCP port bound to the network-instance.
Configurable	False

local-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i>
Description	The local IP address accepted by the application. An all-zeroes value for the ipv4-address means that any IPv4 address is accepted. An all-zeroes value for the ipv6-address means that any IPv6 address is accepted.
Configurable	False

local-port *number*

Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i>
Description	The local port number accepted by the application.
Range	0 to 65535
Configurable	False

process-id *number*

Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> process-id <i>number</i>
Tree	process-id
Description	The process ID of the application that owns the socket.
Configurable	False

statistics

Context	network-instance name <i>string</i> tcp statistics
Tree	statistics
Description	Display statistics
Configurable	False

active-opens *number*

Context	network-instance name <i>string tcp statistics active-opens number</i>
Tree	active-opens
Description	The total number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Default	0
Configurable	False

attempt-fails *number*

Context	network-instance name <i>string tcp statistics attempt-fails number</i>
Tree	attempt-fails
Description	The total number of times that TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times that TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Default	0
Configurable	False

established-resets *number*

Context	network-instance name <i>string tcp statistics established-resets number</i>
Tree	established-resets
Description	The total number of times that TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Default	0
Configurable	False

in-checksum-errors *number*

Context	network-instance name <i>string tcp statistics in-checksum-errors number</i>
Tree	in-checksum-errors
Description	The total number of segments that are received as bad TCP checksum errors.
Default	0
Configurable	False

in-error-segments *number*

Context	network-instance name <i>string</i> tcp statistics in-error-segments <i>number</i>
Tree	in-error-segments
Description	The total number of segments received in error (e.g., bad TCP checksums).
Default	0
Configurable	False

in-segments *number*

Context	network-instance name <i>string</i> tcp statistics in-segments <i>number</i>
Tree	in-segments
Description	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Default	0
Configurable	False

out-rst-segments *number*

Context	network-instance name <i>string</i> tcp statistics out-rst-segments <i>number</i>
Tree	out-rst-segments
Description	The total number of TCP segments sent containing the RST flag.
Default	0
Configurable	False

out-segments *number*

Context	network-instance name <i>string</i> tcp statistics out-segments <i>number</i>
Tree	out-segments
Description	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Default	0
Configurable	False

passive-opens *number*

Context	network-instance name <i>string tcp statistics passive-opens number</i>
Tree	passive-opens
Description	The total number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Default	0
Configurable	False

retransmitted-segments *number*

Context	network-instance name <i>string tcp statistics retransmitted-segments number</i>
Tree	retransmitted-segments
Description	The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Default	0
Configurable	False

type *identityref*

Context	network-instance name <i>string type identityref</i>
Tree	type
Description	The type of network instance. The value of this leaf indicates the type of forwarding entries that should be supported by this network instance
Default	default
Options	<ul style="list-style-type: none">• default A special routing instance which acts as the 'default' or 'global' routing instance for a network device.• ip-vrf A private Layer 3 only routing instance.• mac-vrf A private Layer 2 only switching instance.
Configurable	True

udp

Context	network-instance name <i>string</i> udp
Tree	udp
Description	State for UDP datagrams routed using the route tables of this network instance.
Configurable	False

listening-application **local-address** (*ipv4-address | ipv6-address*) **local-port** *number*

Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i>
Tree	listening-application
Description	List of applications that are listening on a particular UDP port bound to the network-instance.
Configurable	False

local-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i>
Description	The local IP address accepted by the application. An all-zeroes value for the ipv4-address means that any IPv4 address is accepted. An all-zeroes value for the ipv6-address means that any IPv6 address is accepted.
Configurable	False

local-port *number*

Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i>
Description	The local port number accepted by the application.
Range	0 to 65535
Configurable	False

process-id *number*

Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address ipv6-address</i>) local-port <i>number</i> process-id <i>number</i>
Tree	process-id
Description	The process ID of the application that owns the socket.
Configurable	False

statistics

Context	network-instance name <i>string</i> udp statistics
Tree	statistics
Description	Display statistics
Configurable	False

ignored-multicast-packets *number*

Context	network-instance name <i>string</i> udp statistics ignored-multicast-packets <i>number</i>
Tree	ignored-multicast-packets
Description	The total number of ignored multicast UDP datagrams.
Default	0
Configurable	False

in-checksum-errors *number*

Context	network-instance name <i>string</i> udp statistics in-checksum-errors <i>number</i>
Tree	in-checksum-errors
Description	Increased when a received UDP packet has an invalid checksum.
Default	0
Configurable	False

in-error-packets *number*

Context	network-instance name <i>string</i> udp statistics in-error-packets <i>number</i>
Tree	in-error-packets
Description	The total number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Default	0
Configurable	False

in-no-open-ports-packets *number*

Context	network-instance name <i>string</i> udp statistics in-no-open-ports-packets <i>number</i>
Tree	in-no-open-ports-packets
Description	The total number of received UDP datagrams for which there was no application at the destination port.
Default	0
Configurable	False

in-packets *number*

Context	network-instance name <i>string</i> udp statistics in-packets <i>number</i>
Tree	in-packets
Description	The total number of UDP datagrams delivered to UDP users.
Default	0
Configurable	False

out-packets *number*

Context	network-instance name <i>string</i> udp statistics out-packets <i>number</i>
Tree	out-packets
Description	The total number of UDP datagrams sent from this network instance.
Default	0
Configurable	False

receive-buffer-errors *number*

Context	network-instance name <i>string</i> udp statistics receive-buffer-errors <i>number</i>
Tree	receive-buffer-errors
Description	Increased when memory cannot be allocated to process an incoming UDP packet.
Default	0
Configurable	False

send-buffer-errors *number*

Context	network-instance name <i>string</i> udp statistics send-buffer-errors <i>number</i>
Tree	send-buffer-errors
Description	Increased when memory cannot be allocated to send a UDP packet.
Default	0
Configurable	False

6 platform

platform

- **chassis**
 - **clei-code** *string*
 - **failure-reason** *string*
 - **last-booted** *string*
 - **last-change** *string*
 - **mac-address** *string*
 - **manufactured-date** *string*
 - **oper-state** *keyword*
 - **part-number** *string*
 - **power**
 - **control**
 - **allocated** *number*
 - **peak** *number*
 - **used** *number*
 - **fabric**
 - **allocated** *number*
 - **peak** *number*
 - **used** *number*
 - **fan-tray**
 - **allocated** *number*
 - **peak** *number*
 - **used** *number*
 - **linecard**
 - **allocated** *number*
 - **peak** *number*
 - **used** *number*
 - **total**
 - **allocated** *number*
 - **capacity** *number*
 - **peak** *number*
 - **used** *number*
 - **removable** *boolean*
 - **serial-number** *string*
 - **slots** *number*
 - **type** *string*
- **control slot** *string*
 - **clei-code** *string*
 - **cpu index** (*keyword | number*)
 - **architecture** *keyword*
 - **hardware-interrupt**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **idle**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*

-
- **iowait**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **nice**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **software-interrupt**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **speed** *decimal-number*
 - **system**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **total**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **type** *string*
 - **user**
 - **average-1** *number*
 - **average-15** *number*
 - **average-5** *number*
 - **instant** *number*
 - **disk name** *string*
 - **model-number** *string*
 - **partition name** *string*
 - **free** *number*
 - **mount-point** *string*
 - **mount-status** *keyword*
 - **percent-used** *number*
 - **size** *number*
 - **used** *number*
 - **uuid** *string*
 - **serial-number** *string*
 - **size** *number*
 - **statistics**
 - **read-per-second** *decimal-number*
 - **transfers-per-second** *decimal-number*
 - **utilization** *number*
 - **written-per-second** *decimal-number*
 - **type** *keyword*
 - **failure-reason** *string*
 - **last-booted** *string*
 - **last-change** *string*
 - **locator-state** *keyword*

-
- **manufactured-date** *string*
 - **memory**
 - **free** *number*
 - **physical** *number*
 - **reserved** *number*
 - **utilization** *number*
 - **oper-state** *keyword*
 - **part-number** *string*
 - **power**
 - **allocated-power** *number*
 - **used-power** *number*
 - **process pid** *number*
 - **args** *string*
 - **cpu-utilization** *string*
 - **memory-usage** *number*
 - **memory-utilization** *number*
 - **name** *string*
 - **start-time** *string*
 - **removable** *boolean*
 - **role** *keyword*
 - **serial-number** *string*
 - **software-version** *string*
 - **temperature**
 - **alarm-status** *boolean*
 - **instant** *number*
 - **margin** *number*
 - **type** *string*
 - + **fabric slot** *number*
 - + **admin-state** *keyword*
 - **clei-code** *string*
 - **failure-reason** *string*
 - **last-booted** *string*
 - **last-change** *string*
 - **locator-state** *keyword*
 - **manufactured-date** *string*
 - **oper-state** *keyword*
 - **part-number** *string*
 - **power**
 - **allocated-power** *number*
 - **used-power** *number*
 - **removable** *boolean*
 - **serial-number** *string*
 - **temperature**
 - **alarm-status** *boolean*
 - **instant** *number*
 - **margin** *number*
 - **type** *string*
 - **fan-tray id** *number*
 - **clei-code** *string*
 - **failure-reason** *string*
 - **last-booted** *string*
 - **last-change** *string*
 - **locator-state** *keyword*
 - **manufactured-date** *string*

-
- **oper-state** *keyword*
 - **part-number** *string*
 - **power**
 - **allocated-power** *number*
 - **used-power** *number*
 - **removable** *boolean*
 - **serial-number** *string*
 - **speed** *number*
 - **type** *string*
 - + **linecard slot** *number*
 - + **admin-state** *keyword*
 - **clei-code** *string*
 - **failure-reason** *string*
 - + **forwarding-complex name** *keyword*
 - **acl**
 - **resource name** *identityref*
 - **free** *number*
 - **used** *number*
 - **buffer-memory**
 - **dram**
 - **used** *number*
 - **sram**
 - **free** *number*
 - **used** *number*
 - + **fabric**
 - **availability** *number*
 - **utilization-egress** *number*
 - **utilization-ingress** *number*
 - **ip-mpls-forwarding**
 - **resource name** *identityref*
 - **used** *number*
 - **mtu**
 - **resource name** *identityref*
 - **free** *number*
 - **used** *number*
 - **qos**
 - **resource name** *identityref*
 - **free** *number*
 - **used** *number*
 - **tcam**
 - **resource name** *identityref*
 - **free** *number*
 - **programmed** *number*
 - **reserved** *number*
 - **last-booted** *string*
 - **last-change** *string*
 - **locator-state** *keyword*
 - **manufactured-date** *string*
 - **oper-state** *keyword*
 - **part-number** *string*
 - **power**
 - **allocated-power** *number*
 - **used-power** *number*
 - **removable** *boolean*

- **serial-number** *string*
- **software-version** *string*
- **temperature**
 - **alarm-status** *boolean*
 - **instant** *number*
 - **margin** *number*
- **type** *string*
- **power-supply id** *number*
- **capacity** *number*
- **clei-code** *string*
- **failure-reason** *string*
- **input**
 - **current** *decimal-number*
 - **power** *decimal-number*
 - **voltage** *decimal-number*
- **last-booted** *string*
- **last-change** *string*
- **manufactured-date** *string*
- **oper-state** *keyword*
- **part-number** *string*
- **removable** *boolean*
- **serial-number** *string*
- **temperature**
 - **alarm-status** *boolean*
 - **instant** *number*
- **type** *string*
- + **redundancy**
 - **active-module** *keyword*
 - **failover-time** *string*
 - + **synchronization**
 - **last-synchronization** *string*
 - + **overlay**
 - **last-synchronization** *string*
 - **next-synchronization** *string*
 - + **synchronization-frequency** *number*
 - **state** *keyword*
- + **resource-monitoring**
 - + **acl**
 - + **resource name** *identityref*
 - + **falling-threshold-log** *number*
 - + **rising-threshold-log** *number*
 - + **ip-mpls-forwarding**
 - + **resource name** *identityref*
 - + **falling-threshold-log** *number*
 - + **rising-threshold-log** *number*
 - + **mtu**
 - + **resource name** *identityref*
 - + **falling-threshold-log** *number*
 - + **rising-threshold-log** *number*
 - + **qos**
 - + **resource name** *identityref*
 - + **falling-threshold-log** *number*
 - + **rising-threshold-log** *number*
 - + **tcam**

- + **resource name** *identityref*
- + **falling-threshold-log** *number*
- + **rising-threshold-log** *number*

6.1 platform Descriptions

platform

Context	platform
Tree	platform
Description	Enclosing container for platform components
Configurable	True

chassis

Context	platform chassis
Tree	chassis
Description	Top-level container for chassis configuration and state
Configurable	False

clei-code *string*

Context	platform chassis clei-code <i>string</i>
Tree	clei-code
Description	The Common Language Identification Code for this component
Configurable	False

failure-reason *string*

Context	platform chassis failure-reason <i>string</i>
Tree	failure-reason
Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Configurable	False

last-booted *string*

Context	platform chassis last-booted <i>string</i>
Tree	last-booted
Description	The date and time this component last booted

For components that do not boot, this is the time the component was last discovered by the active control module

Configurable False

last-change *string*

Context [platform chassis last-change](#) *string*

Tree [last-change](#)

Description The date and time this component last changed state

Configurable False

mac-address *string*

Context [platform chassis mac-address](#) *string*

Tree [mac-address](#)

Description The chassis MAC address

Configurable False

manufactured-date *string*

Context [platform chassis manufactured-date](#) *string*

Tree [manufactured-date](#)

Description The date this component was manufactured

Configurable False

oper-state *keyword*

Context [platform chassis oper-state](#) *keyword*

Tree [oper-state](#)

Description The operational state of this component

Options

- up
Component or process is operational
- down
Component or process is not operational
- empty
Component slot is empty
- downloading
Component is downloading image into memory

- booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing
Component is currently being synchronized
 - upgrading
Component is currently being upgraded
- Configurable False

part-number *string*

- Context [platform chassis part-number](#) *string*
- Tree [part-number](#)
- Description Part number for this component
- Configurable False

power

- Context [platform chassis power](#)
- Tree [power](#)
- Description Top-level container for chassis-wide power state
- Configurable False

control



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

- Context [platform chassis power control](#)
- Tree [control](#)
- Description Top-level container for power usage of control modules
- Configurable False

allocated *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power control allocated <i>number</i>
Tree	allocated
Description	Allocated power
Configurable	False

peak *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power control peak <i>number</i>
Tree	peak
Description	Peak power used
Configurable	False

used *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power control used <i>number</i>
Tree	used
Description	Used power
Configurable	False

fabric



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fabric
Tree	fabric
Description	Top-level container for power usage of fabric modules
Configurable	False

allocated *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fabric allocated <i>number</i>
Tree	allocated
Description	Allocated power
Configurable	False

peak *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fabric peak <i>number</i>
Tree	peak
Description	Peak power used
Configurable	False

used *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fabric used <i>number</i>
Tree	used
Description	Used power
Configurable	False

fan-tray



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fan-tray
Tree	fan-tray
Description	Top-level container for power usage of fan-trays
Configurable	False

allocated *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fan-tray allocated <i>number</i>
Tree	allocated
Description	Allocated power
Configurable	False

peak *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fan-tray peak <i>number</i>
Tree	peak
Description	Peak power used
Configurable	False

used *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power fan-tray used <i>number</i>
Tree	used
Description	Used power
Configurable	False

linecard



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power linecard
Tree	linecard
Description	Top-level container for power usage of linecard modules
Configurable	False

allocated *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power linecard allocated <i>number</i>
Tree	allocated
Description	Allocated power
Configurable	False

peak *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power linecard peak <i>number</i>
Tree	peak
Description	Peak power used
Configurable	False

used *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power linecard used <i>number</i>
Tree	used
Description	Used power
Configurable	False

total

Context	platform chassis power total
Tree	total
Description	Top-level container for total power usage and capacity
Configurable	False

allocated *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform chassis power total allocated <i>number</i>
Tree	allocated
Description	Allocated power
Configurable	False

capacity *number*

Context	platform chassis power total capacity <i>number</i>
Tree	capacity
Description	Total power capacity provided by all power supplies
Configurable	False

peak *number*

Context	platform chassis power total peak <i>number</i>
Tree	peak
Description	Peak power used
Configurable	False

used *number*

Context	platform chassis power total used <i>number</i>
Tree	used
Description	Used power
Configurable	False

removable *boolean*

Context	platform chassis removable <i>boolean</i>
Tree	removable
Description	Details if this component can be removed from the system
Configurable	False

serial-number *string*

Context	platform chassis serial-number <i>string</i>
Tree	serial-number
Description	The serial number for this component
Configurable	False

slots *number*

Context	platform chassis slots <i>number</i>
Tree	slots
Description	The number of line card slots supported by the chassis
Configurable	False

type *string*

Context	platform chassis type <i>string</i>
Tree	type
Description	The chassis type
Configurable	False

control slot *string*

Context	platform control slot <i>string</i>
Tree	control
Description	Top-level container for control module configuration and state
Configurable	False

slot *string*

Context	platform control slot <i>string</i>
Description	Slot identifier for the control module This is set to 'A' for systems without removable control modules.
Configurable	False

clei-code *string*

Context	platform control slot <i>string</i> clei-code <i>string</i>
Tree	clei-code
Description	The Common Language Identification Code for this component
Configurable	False

cpu index (*keyword | number*)

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>)
Tree	cpu
Description	List of all CPUs in the system
Configurable	False

index (*keyword | number*)

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>)
Description	CPU index for each processor core on the system On a single-core system, the index should be zero. The 'all' index signifies an aggregation of the CPU utilization statistics over all cores in the system.
Options	<ul style="list-style-type: none">all Index value indicating all CPUs in the system
Configurable	False

architecture *keyword*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) architecture <i>keyword</i>
Tree	architecture
Description	Architecture supported by the CPU
Options	<ul style="list-style-type: none">x86_64
Configurable	False

hardware-interrupt

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt
Tree	hardware-interrupt
Description	Time spent servicing hardware interrupts
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

idle

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) idle
Tree	idle
Description	Time spent idle
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) idle average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) idle average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) idle average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) idle instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

iowait

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) iowait
Tree	iowait
Description	Time spent idle, waiting for an outstanding disk I/O request
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) iowait average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) iowait average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) iowait average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) iowait instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

nice

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) nice
Tree	nice
Description	Time spent running low-priority (niced) user processes
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) nice average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) nice average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) nice average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) nice instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

software-interrupt

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt
Tree	software-interrupt
Description	Time spent servicing software interrupts
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

speed *decimal-number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) speed <i>decimal-number</i>
Tree	speed
Description	Capable speed of the CPU
Units	megahertz
Configurable	False

system

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system
Tree	system
Description	Time spent executing at the system level This can otherwise be known as kernel time, and does not include time spent servicing hardware and software interrupts.
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

total

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total
Tree	total
Description	Total CPU utilization
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

type *string*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) type <i>string</i>
Tree	type
Description	Model name of the CPU
Configurable	False

user

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) user
Tree	user
Description	Time spent executing at the user level This can otherwise be known as application or user space time.
Configurable	False

average-1 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) user average-1 <i>number</i>
Tree	average-1
Description	The arithmetic mean value of this statistic over the last minute
Range	0 to 100
Configurable	False

average-15 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) user average-15 <i>number</i>
Tree	average-15
Description	The arithmetic mean value of this statistic over the last fifteen minutes
Range	0 to 100
Configurable	False

average-5 *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) user average-5 <i>number</i>
Tree	average-5
Description	The arithmetic mean value of this statistic over the last five minutes
Range	0 to 100
Configurable	False

instant *number*

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) user instant <i>number</i>
Tree	instant
Description	The instantaneous percentage value
Range	0 to 100
Configurable	False

disk name *string*

Context	platform control slot <i>string</i> disk name <i>string</i>
Tree	disk
Description	List of disks present in the system
Configurable	False

name *string*

Context	platform control slot <i>string</i> disk name <i>string</i>
Description	Name of the disk, as defined by its physical location in the system
Configurable	False

model-number *string*

Context	platform control slot <i>string</i> disk name <i>string</i> model-number <i>string</i>
Tree	model-number
Description	Model name of the disk
Configurable	False

partition name *string*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i>
Tree	partition
Description	List of partitions available on this disk
Configurable	False

name *string*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i>
Description	Name of the partition
Configurable	False

free *number*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> free <i>number</i>
Tree	free
Description	Space free on the partition
Units	bytes
Configurable	False

mount-point *string*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> mount-point <i>string</i>
Tree	mount-point
Description	Path to where this partition is mounted
Configurable	False

mount-status *keyword*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> mount-status <i>keyword</i>
Tree	mount-status
Description	Current mount status of this partition
Options	<ul style="list-style-type: none">• ro Partition is currently mounted read-only• rw Partition is currently mounted read-write
Configurable	False

percent-used *number*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> percent-used <i>number</i>
Tree	percent-used
Description	Percentage of the partition in use
Range	0 to 100
Configurable	False

size *number*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> size <i>number</i>
Tree	size
Description	Size of the partition
Units	bytes
Configurable	False

used *number*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> used <i>number</i>
Tree	used
Description	Space used on the partition
Units	bytes
Configurable	False

uuid *string*

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> uuid <i>string</i>
Tree	uuid
Description	UUID of the partition
Configurable	False

serial-number *string*

Context	platform control slot <i>string</i> disk name <i>string</i> serial-number <i>string</i>
Tree	serial-number
Description	Serial number of the disk
Configurable	False

size *number*

Context	platform control slot <i>string</i> disk name <i>string</i> size <i>number</i>
Tree	size
Description	Total size of the disk
Configurable	False

statistics

Context	platform control slot <i>string</i> disk name <i>string</i> statistics
Tree	statistics
Description	Top-level container for disk statistics
Configurable	False

read-per-second *decimal-number*

Context	platform control slot <i>string</i> disk name <i>string</i> statistics read-per-second <i>decimal-number</i>
Tree	read-per-second
Description	Indicates the amount of data read from the device per second
Units	bytes
Configurable	False

transfers-per-second *decimal-number*

Context	platform control slot <i>string</i> disk name <i>string</i> statistics transfers-per-second <i>decimal-number</i>
Tree	transfers-per-second
Description	Indicates the number of transfers per second that were issued to the device. A transfer is an I/O request to the device. Multiple logical requests can be combined into a single I/O request to the device. A transfer is of indeterminate size.
Configurable	False

utilization *number*

Context	platform control slot <i>string</i> disk name <i>string</i> statistics utilization <i>number</i>
Tree	utilization
Description	The current tps utilization of the disk, expressed as a percentage
Range	0 to 100
Configurable	False

written-per-second *decimal-number*

Context	platform control slot <i>string</i> disk name <i>string</i> statistics written-per-second <i>decimal-number</i>
Tree	written-per-second
Description	Indicates the amount of data written to the device per second
Units	bytes
Configurable	False

type *keyword*

Context	platform control slot <i>string</i> disk name <i>string</i> type <i>keyword</i>
Tree	type
Description	Type of disk
Options	<ul style="list-style-type: none">• compactflash• ssd• hdd• usb
Configurable	False

failure-reason *string*

Context	platform control slot <i>string</i> failure-reason <i>string</i>
Tree	failure-reason
Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Configurable	False

last-booted *string*

Context	platform control slot <i>string</i> last-booted <i>string</i>
Tree	last-booted
Description	The date and time this component last booted For components that do not boot, this is the time the component was last discovered by the active control module
Configurable	False

last-change *string*

Context	platform control slot <i>string</i> last-change <i>string</i>
Tree	last-change
Description	The date and time this component last changed state
Configurable	False

locator-state *keyword*

Context	platform control slot <i>string</i> locator-state <i>keyword</i>
Tree	locator-state
Description	Details if the locator LED is active on this component
Default	inactive
Options	<ul style="list-style-type: none">• active Locator LED is currently active• inactive Locator LED is currently inactive
Configurable	False

manufactured-date *string*

Context	platform control slot <i>string</i> manufactured-date <i>string</i>
Tree	manufactured-date
Description	The date this component was manufactured
Configurable	False

memory

Context	platform control slot <i>string</i> memory
Tree	memory
Description	Top-level container for system memory state
Configurable	False

free *number*

Context	platform control slot <i>string</i> memory free <i>number</i>
Tree	free
Description	Memory available for system use
Units	bytes
Configurable	False

physical *number*

Context	platform control slot <i>string</i> memory physical <i>number</i>
Tree	physical
Description	Total physical memory available on this component
Units	bytes
Configurable	False

reserved *number*

Context	platform control slot <i>string</i> memory reserved <i>number</i>
Tree	reserved
Description	Memory reserved for system use
Units	bytes
Configurable	False

utilization *number*

Context	platform control slot <i>string</i> memory utilization <i>number</i>
Tree	utilization
Description	Total memory utilized
Range	0 to 100
Configurable	False

oper-state *keyword*

Context	platform control slot <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of this component
Options	<ul style="list-style-type: none">• up

- Component or process is operational
 - down
 - Component or process is not operational
 - empty
 - Component slot is empty
 - downloading
 - Component is downloading image into memory
 - booting
 - Component is booting downloaded image
 - starting
 - Component image operational, application processes starting
 - failed
 - Component or process has failed
 - synchronizing
 - Component is currently being synchronized
 - upgrading
 - Component is currently being upgraded
- Configurable False

part-number *string*

- Context **platform control slot** *string* **part-number** *string*
- Tree **part-number**
- Description Part number for this component
- Configurable False

power

- Context **platform control slot** *string* **power**
- Tree **power**
- Description State related to power consumption and allocation for this component
- Configurable False

allocated-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform control slot <i>string</i> power allocated-power <i>number</i>
Tree	allocated-power
Description	The power budget allocated to this component
Units	watts
Configurable	False

used-power *number*

Context	platform control slot <i>string</i> power used-power <i>number</i>
Tree	used-power
Description	The power in use by this component
Units	watts
Configurable	False

process pid *number*

Context	platform control slot <i>string</i> process pid <i>number</i>
Tree	process
Description	List of system processes
Configurable	False

pid *number*

Context	platform control slot <i>string</i> process pid <i>number</i>
Description	The process ID
Configurable	False

args *string*

Context	platform control slot <i>string</i> process pid <i>number</i> args <i>string</i>
Tree	args
Description	Current process command line arguments Arguments with a parameter (e.g., --option 10 or -option=10) should be represented as a single element of the list with the argument name and parameter together. Flag arguments, i.e., those without a parameter should also be in their own list element.
Configurable	False

cpu-utilization *string*

Context	platform control slot <i>string</i> process pid <i>number</i> cpu-utilization <i>string</i>
Tree	cpu-utilization
Description	The percentage of CPU that is being used by the process
Configurable	False

memory-usage *number*

Context	platform control slot <i>string</i> process pid <i>number</i> memory-usage <i>number</i>
Tree	memory-usage
Description	Bytes allocated and still in use by the process
Units	bytes
Configurable	False

memory-utilization *number*

Context	platform control slot <i>string</i> process pid <i>number</i> memory-utilization <i>number</i>
Tree	memory-utilization
Description	The percentage of RAM that is being used by the process
Range	0 to 100
Configurable	False

name *string*

Context	platform control slot <i>string</i> process pid <i>number</i> name <i>string</i>
Tree	name
Description	The process name
Configurable	False

start-time *string*

Context	platform control slot <i>string</i> process pid <i>number</i> start-time <i>string</i>
Tree	start-time
Description	The time at which this process started
Configurable	False

removable *boolean*

Context	platform control slot <i>string</i> removable <i>boolean</i>
Tree	removable
Description	Details if this component can be removed from the system
Configurable	False

role *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform control slot <i>string</i> role <i>keyword</i>
Tree	role
Description	Control module role, detailing active or standby state This field is not present on systems without removable control modules.
Options	<ul style="list-style-type: none">• active• standby
Configurable	False

serial-number *string*

Context	platform control slot <i>string</i> serial-number <i>string</i>
Tree	serial-number
Description	The serial number for this component
Configurable	False

software-version *string*

Context	platform control slot <i>string</i> software-version <i>string</i>
Tree	software-version
Description	Image version version running on this component This version is the squashfs version, and may not represent the current per-application versions if versions have been modified after the system has been installed.
Configurable	False

temperature

Context	platform control slot <i>string</i> temperature
Tree	temperature
Description	State related to temperature for this component
Configurable	False

alarm-status *boolean*

Context	platform control slot <i>string</i> temperature alarm-status <i>boolean</i>
Tree	alarm-status
Description	Indicates if a temperature sensor of this component is currently in an alarm state An alarm state is triggered if the margin field is ≤ 2 degrees, indicating that a thermal protection shut down is imminent unless adequate system cooling is provided to bring the temperature sensor back into safe operating ranges.
Configurable	False

instant *number*

Context	platform control slot <i>string</i> temperature instant <i>number</i>
Tree	instant
Description	Represents the highest temperature of any sensor on this component Note that as multiple sensors may feed in, that this field and the margin field may be referencing different sensors.
Configurable	False

margin *number*

Context	platform control slot <i>string</i> temperature margin <i>number</i>
Tree	margin
Description	Indicates the lowest alarm margin of any sensor on this component The margin is the delta between the current sensor temperature and the thermal protection threshold for that sensor. Note that as multiple sensors may feed in, that this field and the instant field may be referencing different sensors.
Configurable	False

type *string*

Context	platform control slot <i>string type string</i>
Tree	type
Description	Control module type, as translated from the components EEPROM
Configurable	False

fabric slot *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i>
Tree	fabric
Description	Top-level container for fabric configuration and state
Configurable	True

slot *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i>
Description	Numeric identifier for the fabric module
Range	1 to 255
Configurable	True

admin-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> admin-state <i>keyword</i>
Tree	admin-state
Description	The administrative state of this component
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

clei-code *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> clei-code <i>string</i>
Tree	clei-code
Description	The Common Language Identification Code for this component
Configurable	False

failure-reason *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> failure-reason <i>string</i>
Tree	failure-reason
Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Configurable	False

last-booted *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> last-booted <i>string</i>
Tree	last-booted
Description	The date and time this component last booted For components that do not boot, this is the time the component was last discovered by the active control module
Configurable	False

last-change *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> last-change <i>string</i>
Tree	last-change
Description	The date and time this component last changed state
Configurable	False

locator-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> locator-state <i>keyword</i>
Tree	locator-state
Description	Details if the locator LED is active on this component
Default	inactive
Options	<ul style="list-style-type: none">• active Locator LED is currently active• inactive Locator LED is currently inactive
Configurable	False

manufactured-date *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> manufactured-date <i>string</i>
Tree	manufactured-date
Description	The date this component was manufactured
Configurable	False

oper-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of this component
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading

Component is currently being upgraded

Configurable False

part-number *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **platform fabric slot** *number* **part-number** *string*

Tree **part-number**

Description Part number for this component

Configurable False

power



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **platform fabric slot** *number* **power**

Tree **power**

Description State related to power consumption and allocation for this component

Configurable False

allocated-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **platform fabric slot** *number* **power allocated-power** *number*

Tree **allocated-power**

Description The power budget allocated to this component

Units watts

Configurable False

used-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> power used-power <i>number</i>
Tree	used-power
Description	The power in use by this component
Units	watts
Configurable	False

removable *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> removable <i>boolean</i>
Tree	removable
Description	Details if this component can be removed from the system
Configurable	False

serial-number *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> serial-number <i>string</i>
Tree	serial-number
Description	The serial number for this component
Configurable	False

temperature



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> temperature
Tree	temperature
Description	State related to temperature for this component
Configurable	False

alarm-status *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> temperature alarm-status <i>boolean</i>
Tree	alarm-status
Description	Indicates if a temperature sensor of this component is currently in an alarm state An alarm state is triggered if the margin field is ≤ 2 degrees, indicating that a thermal protection shut down is imminent unless adequate system cooling is provided to bring the temperature sensor back into safe operating ranges.
Configurable	False

instant *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> temperature instant <i>number</i>
Tree	instant
Description	Represents the highest temperature of any sensor on this component Note that as multiple sensors may feed in, that this field and the margin field may be referencing different sensors.
Configurable	False

margin *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> temperature margin <i>number</i>
Tree	margin
Description	Indicates the lowest alarm margin of any sensor on this component The margin is the delta between the current sensor temperature and the thermal protection threshold for that sensor. Note that as multiple sensors may feed in, that this field and the instant field may be referencing different sensors.
Configurable	False

type *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot <i>number</i> type <i>string</i>
Tree	type
Description	Fabric module type, as translated from the components EEPROM
Configurable	False

fan-tray **id** *number*

Context	platform fan-tray id <i>number</i>
Tree	fan-tray
Description	Top-level container for fan module configuration and state
Configurable	False

id *number*

Context	platform fan-tray id <i>number</i>
Description	Numeric identifier for the fan tray
Range	1 to 255
Configurable	False

clei-code *string*

Context	platform fan-tray id <i>number clei-code string</i>
Tree	clei-code
Description	The Common Language Identification Code for this component
Configurable	False

failure-reason *string*

Context	platform fan-tray id <i>number failure-reason string</i>
Tree	failure-reason
Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Configurable	False

last-booted *string*

Context	platform fan-tray id <i>number last-booted string</i>
Tree	last-booted
Description	The date and time this component last booted For components that do not boot, this is the time the component was last discovered by the active control module
Configurable	False

last-change *string*

Context	platform fan-tray id <i>number last-change string</i>
Tree	last-change
Description	The date and time this component last changed state
Configurable	False

locator-state *keyword*

Context	platform fan-tray id <i>number locator-state keyword</i>
Tree	locator-state
Description	Details if the locator LED is active on this component
Default	inactive
Options	<ul style="list-style-type: none">• active

	Locator LED is currently active
	• inactive
	Locator LED is currently inactive
Configurable	False

manufactured-date *string*

Context	platform fan-tray id <i>number</i> manufactured-date <i>string</i>
Tree	manufactured-date
Description	The date this component was manufactured
Configurable	False

oper-state *keyword*

Context	platform fan-tray id <i>number</i> oper-state <i>keyword</i>
Tree	oper-state
Description	The operational state of this component
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

part-number *string*

Context	platform fan-tray id number part-number <i>string</i>
Tree	part-number
Description	Part number for this component
Configurable	False

power



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fan-tray id number power
Tree	power
Description	State related to power consumption and allocation for this component
Configurable	False

allocated-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fan-tray id number power allocated-power <i>number</i>
Tree	allocated-power
Description	The power budget allocated to this component
Units	watts
Configurable	False

used-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fan-tray id <i>number</i> power used-power <i>number</i>
Tree	used-power
Description	The power in use by this component
Units	watts
Configurable	False

removable *boolean*

Context	platform fan-tray id <i>number</i> removable <i>boolean</i>
Tree	removable
Description	Details if this component can be removed from the system
Configurable	False

serial-number *string*

Context	platform fan-tray id <i>number</i> serial-number <i>string</i>
Tree	serial-number
Description	The serial number for this component
Configurable	False

speed *number*

Context	platform fan-tray id <i>number</i> speed <i>number</i>
Tree	speed
Description	The current speed of the fan tray
Range	0 to 100
Configurable	False

type *string*

Context	platform fan-tray id <i>number</i> type <i>string</i>
Tree	type
Description	Fan tray type, as translated from the components EEPROM
Configurable	False

linecard slot *number*

Context	platform linecard slot number
Tree	linecard
Description	Top-level container for linecard configuration and state
Configurable	True

slot *number*

Context	platform linecard slot number
Description	Numeric identifier for the linecard
Range	1 to 8
Configurable	True

admin-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number admin-state keyword
Tree	admin-state
Description	The administrative state of this component
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

clei-code *string*

Context	platform linecard slot number clei-code string
Tree	clei-code
Description	The Common Language Identification Code for this component
Configurable	False

failure-reason *string*

Context	platform linecard slot number failure-reason <i>string</i>
Tree	failure-reason
Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Configurable	False

forwarding-complex **name** *keyword*

Context	platform linecard slot number forwarding-complex name <i>keyword</i>
Tree	forwarding-complex
Description	List of forwarding complexes on the linecard
Configurable	True

name *keyword*

Context	platform linecard slot number forwarding-complex name <i>keyword</i>
Description	The identifier of the forwarding complex
Options	• 0
Configurable	True

acl

Context	platform linecard slot number forwarding-complex name <i>keyword</i> acl
Tree	acl
Description	Access control list
Configurable	False

resource **name** *identityref*

Context	platform linecard slot number forwarding-complex name <i>keyword</i> acl resource name <i>identityref</i>
Tree	resource
Description	ACL resource
Configurable	False

name *identityref*

Context	platform linecard slot number forwarding-complex name <i>keyword acl resource name identityref</i>
Description	The name of the ACL resource
Options	<ul style="list-style-type: none">input-ipv4-filter-instances An input-ipv4-filter-instance resource is used every time an IPv4 filter instance is created and applied to ingress traffic on the forwarding complex. Only one instance is used if the subinterface-specific property of the filter is set to output-only; otherwise one instance is used for every subinterface using the IPv4 filter.input-ipv6-filter-instances An input-ipv6-filter-instance resource is used every time an IPv6 filter instance is created and applied to ingress traffic on the forwarding complex. Only one instance is used if the subinterface-specific property of the filter is set to output-only; otherwise one instance is used for every subinterface using the IPv6 filter.
Configurable	False

free *number*

Context	platform linecard slot number forwarding-complex name <i>keyword acl resource name identityref free number</i>
Tree	free
Description	The number of resources that are unused and available
Configurable	False

used *number*

Context	platform linecard slot number forwarding-complex name <i>keyword acl resource name identityref used number</i>
Tree	used
Description	The number of resources that are in use
Configurable	False

buffer-memory

Context	platform linecard slot number forwarding-complex name <i>keyword buffer-memory</i>
Tree	buffer-memory
Description	Container for utilization statistics of the packet buffer memory
Configurable	False

dram

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> buffer-memory dram
Tree	dram
Description	Container for utilization statistics of the DRAM memory.
Configurable	False

used number

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> buffer-memory dram used <i>number</i>
Tree	used
Description	Used DRAM memory
Range	0 to 100
Configurable	False

sram

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> buffer-memory sram
Tree	sram
Description	Container for utilization statistics of the on-chip SRAM memory.
Configurable	False

free number

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> buffer-memory sram free <i>number</i>
Tree	free
Description	Available SRAM memory
Units	bytes
Configurable	False

used *number*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> buffer-memory sram used <i>number</i>
Tree	used
Description	Used SRAM memory
Units	bytes
Configurable	False

fabric



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> fabric
Tree	fabric
Description	Top-level container for fabric configuration and state
Configurable	True

availability *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> fabric availability <i>number</i>
Tree	availability
Description	Details the percentage bandwidth available to the fabric for the line card
Range	0 to 100
Configurable	False

utilization-egress *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword fabric</i> utilization-egress <i>number</i>
Tree	utilization-egress
Description	Provides the linecard bandwidth utilization from the switch fabric
Configurable	False

utilization-ingress *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword fabric</i> utilization-ingress <i>number</i>
Tree	utilization-ingress
Description	Provides the linecard bandwidth utilization into the switch fabric
Configurable	False

ip-mpls-forwarding

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword ip-mpls-forwarding</i>
Tree	ip-mpls-forwarding
Description	
Configurable	False

resource **name** *identityref*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword ip-mpls-forwarding</i> resource name <i>identityref</i>
Tree	resource
Description	
Configurable	False

name *identityref*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> ip-mpls-forwarding resource name <i>identityref</i>
Description	The name of the IP-MPLS forwarding resource
Options	<ul style="list-style-type: none">• ip-fib Each IP route (ECMP or non-ECMP) to an IPv4 or IPv6 prefix uses one of these resources. The underlying resource in J2 is the KAPS1 table.• ip-arp-nd Each IPv4 ARP entry and each IPv6 neighbor entry uses one of these resources.• direct-next-hops Each direct next-hop in a next-hop-group (static or dynamic) uses one of these resources. A direct next-hop is resolved by a local interface route. The same direct next-hop in two different NHGs still counts as one direct next-hop.• indirect-next-hops Each indirect next-hop in a next-hop-group (static or dynamic) uses one of these resources. An indirect next-hop is resolved by any route other than a local interface route. The same indirect next-hop in two different NHGs still counts as one indirect next-hop.• hardware-ecmp-fecs This represents the pool of resources used to support ECMP forwarding in hardware. On a J2 IMM the utilization for this pool of resources is calculated as the maximum utilization of the following tables: L1 ECMP FECs, L2 ECMP FECs, L1 ECMP member FECs and L2 ECMP member FECs• hardware-fecs This represents the pool of resources used to support non-ECMP forwarding in hardware. On a J2 IMM the utilization for this pool of resources is calculated as the maximum utilization of the following tables: L1 non-ECMP FECs, L2 non-ECMP FECs.
Configurable	False

used *number*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> ip-mpls-forwarding resource name <i>identityref</i> used <i>number</i>
Tree	used
Description	The percentage of the resource that is currently used
Range	0 to 100
Configurable	False

mtu

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> mtu
Tree	mtu
Description	
Configurable	False

resource **name** *identityref*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> mtu resource name <i>identityref</i>
Tree	resource
Description	
Configurable	False

name *identityref*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> mtu resource name <i>identityref</i>
Description	The name of the MTU resource
Options	<ul style="list-style-type: none">• ip-mtu IP MTU resource pool. One resource from this pool is consumed by every different IP MTU value used by the subinterfaces on the linecard forwarding-complex.• port-mtu Port MTU resource pool. One resource from this pool is consumed by every different port MTU value used by a port on the linecard forwarding-complex.
Configurable	False

free *number*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> mtu resource name <i>identityref</i> free <i>number</i>
Tree	free
Description	The number of resources that are unused and available
Configurable	False

used *number*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> mtu resource name <i>identityref</i> used <i>number</i>
Tree	used
Description	The number of resources that are in use
Configurable	False

qos

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> qos
Tree	qos
Description	
Configurable	False

resource name *identityref*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> qos resource name <i>identityref</i>
Tree	resource
Description	
Configurable	False

name *identityref*

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> qos resource name <i>identityref</i>
Description	The name of the QoS resource
Options	<ul style="list-style-type: none">• classifier-profiles A classifier-profile resource is used every time a different combination of DSCP classifier and MPLS-TC classifier is applied to an ingress subinterface of the forwarding complex. There are 16 of these resources and one is always used by the combination of the default DSCP classifier and the default MPLS TC classifier.• rewrite-profiles A rewrite-profile resource is used every time a different combination of DSCP rewrite-rule and MPLS-TC rewrite-rule is applied to an egress subinterface of the forwarding complex. There are 32 of these resources.
Configurable	False

free number

Context	platform linecard slot number forwarding-complex name <i>keyword qos resource name identityref free number</i>
Tree	free
Description	The number of resources that are unused and available
Configurable	False

used number

Context	platform linecard slot number forwarding-complex name <i>keyword qos resource name identityref used number</i>
Tree	used
Description	The number of resources that are in use
Configurable	False

tcam

Context	platform linecard slot number forwarding-complex name <i>keyword tcam</i>
Tree	tcam
Description	
Configurable	False

resource name *identityref*

Context	platform linecard slot number forwarding-complex name <i>keyword tcam resource name identityref</i>
Tree	resource
Description	
Configurable	False

name *identityref*

Context	platform linecard slot number forwarding-complex name <i>keyword tcam resource name identityref</i>
Description	The name of the TCAM resource
Options	<ul style="list-style-type: none">if-input-ipv4 Resource pool of TCAM entries used by IPv4 ACLs applied as subinterface-input filersif-output-ipv4

- Resource pool of TCAM entries used by IPv4 ACLs applied as subinterface-output filters
 - if-input-ipv6
 - Resource pool of TCAM entries used by IPv6 ACLs applied as subinterface-input filters
 - if-output-ipv6
 - Resource pool of TCAM entries used by IPv6 ACLs applied as subinterface-output filters
 - cpm-capture-ipv4
 - Resource pool of TCAM entries used by IPv4 cpm-filter ACLs and capture-filter ACLs
 - cpm-capture-ipv6
 - Resource pool of TCAM entries used by IPv6 cpm-filter ACLs and capture-filter ACLs
- Configurable False

free number

- Context **platform linecard slot** *number* **forwarding-complex name** *keyword* **tcam resource name** *identityref* **free number**
- Tree **free**
- Description The number of available, unused TCAM entries remaining in this resource pool
- Configurable False

programmed number

- Context **platform linecard slot** *number* **forwarding-complex name** *keyword* **tcam resource name** *identityref* **programmed number**
- Tree **programmed**
- Description The number of TCAM entries belonging to this resource that are currently programmed into hardware. When the number of programmed entries equals the number of reserved entries HW programming of this resource type has finished.
- Configurable False

reserved number

- Context **platform linecard slot** *number* **forwarding-complex name** *keyword* **tcam resource name** *identityref* **reserved number**
- Tree **reserved**
- Description The number of TCAM entries that are currently reserved in this resource pool. Reservation happens when a configuration change is committed. Reserved entries may not be programmed yet if the commit has just occurred.
- Configurable False

last-booted *string*

Context	platform linecard slot <i>number last-booted string</i>
Tree	last-booted
Description	The date and time this component last booted For components that do not boot, this is the time the component was last discovered by the active control module
Configurable	False

last-change *string*

Context	platform linecard slot <i>number last-change string</i>
Tree	last-change
Description	The date and time this component last changed state
Configurable	False

locator-state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number locator-state keyword</i>
Tree	locator-state
Description	Details if the locator LED is active on this component
Default	inactive
Options	<ul style="list-style-type: none">• active Locator LED is currently active• inactive Locator LED is currently inactive
Configurable	False

manufactured-date *string*

Context	platform linecard slot <i>number manufactured-date string</i>
Tree	manufactured-date
Description	The date this component was manufactured
Configurable	False

oper-state *keyword*

Context	platform linecard slot <i>number oper-state keyword</i>
Tree	oper-state
Description	The operational state of this component
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

part-number *string*

Context	platform linecard slot <i>number part-number string</i>
Tree	part-number
Description	Part number for this component
Configurable	False

power



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number power
Tree	power
Description	State related to power consumption and allocation for this component
Configurable	False

allocated-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number power allocated-power number
Tree	allocated-power
Description	The power budget allocated to this component
Units	watts
Configurable	False

used-power *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number power used-power number
Tree	used-power
Description	The power in use by this component
Units	watts
Configurable	False

removable *boolean*

Context	platform linecard slot number removable boolean
Tree	removable
Description	Details if this component can be removed from the system
Configurable	False

serial-number *string*

Context	platform linecard slot <i>number</i> serial-number <i>string</i>
Tree	serial-number
Description	The serial number for this component
Configurable	False

software-version *string*

Context	platform linecard slot <i>number</i> software-version <i>string</i>
Tree	software-version
Description	Image version version running on this component This version is the squashfs version, and may not represent the current per-application versions if versions have been modified after the system has been installed.
Configurable	False

temperature



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> temperature
Tree	temperature
Description	State related to temperature for this component
Configurable	False

alarm-status *boolean*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> temperature alarm-status <i>boolean</i>
Tree	alarm-status
Description	Indicates if a temperature sensor of this component is currently in an alarm state

An alarm state is triggered if the margin field is ≤ 2 degrees, indicating that a thermal protection shut down is imminent unless adequate system cooling is provided to bring the temperature sensor back into safe operating ranges.

Configurable False

instant *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **platform linecard slot** *number* **temperature instant** *number*

Tree **instant**

Description Represents the highest temperature of any sensor on this component
Note that as multiple sensors may feed in, that this field and the margin field may be referencing different sensors.

Configurable False

margin *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context **platform linecard slot** *number* **temperature margin** *number*

Tree **margin**

Description Indicates the lowest alarm margin of any sensor on this component
The margin is the delta between the current sensor temperature and the thermal protection threshold for that sensor. Note that as multiple sensors may feed in, that this field and the instant field may be referencing different sensors.

Configurable False

type *string*

Context **platform linecard slot** *number* **type** *string*

Tree **type**

Description Linecard type, as translated from the components EEPROM

Configurable False

power-supply id *number*

Context	platform power-supply id <i>number</i>
Tree	power-supply
Description	Top-level container for power supply module configuration and state
Configurable	False

id *number*

Context	platform power-supply id <i>number</i>
Description	Numeric identifier for the power supply module
Range	1 to 255
Configurable	False

capacity *number*

Context	platform power-supply id <i>number</i> capacity <i>number</i>
Tree	capacity
Description	The total capacity the power supply module can provide
Units	watts
Configurable	False

clei-code *string*

Context	platform power-supply id <i>number</i> clei-code <i>string</i>
Tree	clei-code
Description	The Common Language Identification Code for this component
Configurable	False

failure-reason *string*

Context	platform power-supply id <i>number</i> failure-reason <i>string</i>
Tree	failure-reason
Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Configurable	False

input

Context	platform power-supply id <i>number</i> input
Tree	input
Description	Top-level container for power-supply input state
Configurable	False

current *decimal-number*

Context	platform power-supply id <i>number</i> input current <i>decimal-number</i>
Tree	current
Description	Current input amperage for the power-supply
Units	amps
Configurable	False

power *decimal-number*

Context	platform power-supply id <i>number</i> input power <i>decimal-number</i>
Tree	power
Description	Current input power for the power-supply
Units	watts
Configurable	False

voltage *decimal-number*

Context	platform power-supply id <i>number</i> input voltage <i>decimal-number</i>
Tree	voltage
Description	Current input voltage for the power-supply
Units	volts
Configurable	False

last-booted *string*

Context	platform power-supply id <i>number</i> last-booted <i>string</i>
Tree	last-booted
Description	The date and time this component last booted

For components that do not boot, this is the time the component was last discovered by the active control module

Configurable False

last-change *string*

Context **platform power-supply id** *number last-change string*

Tree **last-change**

Description The date and time this component last changed state

Configurable False

manufactured-date *string*

Context **platform power-supply id** *number manufactured-date string*

Tree **manufactured-date**

Description The date this component was manufactured

Configurable False

oper-state *keyword*

Context **platform power-supply id** *number oper-state keyword*

Tree **oper-state**

Description The operational state of this component

- Options
- up
Component or process is operational
 - down
Component or process is not operational
 - empty
Component slot is empty
 - downloading
Component is downloading image into memory
 - booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing

	Component is currently being synchronized
	• upgrading
	Component is currently being upgraded
Configurable	False

part-number *string*

Context	platform power-supply id <i>number</i> part-number <i>string</i>
Tree	part-number
Description	Part number for this component
Configurable	False

removable *boolean*

Context	platform power-supply id <i>number</i> removable <i>boolean</i>
Tree	removable
Description	Details if this component can be removed from the system
Configurable	False

serial-number *string*

Context	platform power-supply id <i>number</i> serial-number <i>string</i>
Tree	serial-number
Description	The serial number for this component
Configurable	False

temperature

Context	platform power-supply id <i>number</i> temperature
Tree	temperature
Description	State related to temperature for this component
Configurable	False

alarm-status *boolean*

Context	platform power-supply id <i>number</i> temperature alarm-status <i>boolean</i>
Tree	alarm-status
Description	Indicates if the temperature of this component is currently in an alarm state
Configurable	False

instant *number*

Context	platform power-supply id <i>number</i> temperature instant <i>number</i>
Tree	instant
Description	The current temperature of this component
Configurable	False

type *string*

Context	platform power-supply id <i>number</i> type <i>string</i>
Tree	type
Description	Power-supply type, as translated from the components EEPROM
Configurable	False

redundancy



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy
Tree	redundancy
Description	Top-level container for platform redundancy
Configurable	True

active-module *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy active-module <i>keyword</i>
Tree	active-module
Description	Control module currently active
Options	<ul style="list-style-type: none">• A• B
Configurable	False

failover-time *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy failover-time <i>string</i>
Tree	failover-time
Description	Date and time of the last control module failover
Configurable	False

synchronization



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization
Tree	synchronization
Description	Top-level container for redundancy synchronization
Configurable	True

last-synchronization *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization last-synchronization <i>string</i>
Tree	last-synchronization
Description	Last date and time a synchronization of system files occurred
Configurable	False

overlay



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization overlay
Tree	overlay
Description	Top-level container for overlay synchronization
Configurable	True

last-synchronization *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization overlay last-synchronization <i>string</i>
Tree	last-synchronization
Description	Last date and time a synchronization of the overlay occurred
Configurable	False

next-synchronization *string*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization overlay next-synchronization <i>string</i>
Tree	next-synchronization
Description	Next date and time a synchronization of the overlay will occur
Configurable	False

synchronization-frequency *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization overlay synchronization-frequency <i>number</i>
Tree	synchronization-frequency
Description	Sets the frequency of overlay synchronizations This has no effect if overlay is not a configured synchronization mode. Changing this value results in the timer to the next synchronization being reset.
Range	30 to 65535
Default	60
Units	seconds
Configurable	True

state *keyword*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronization state <i>keyword</i>
Tree	state
Description	Current synchronization status
Options	<ul style="list-style-type: none">• synchronized Standby control module is ready and synchronized• synchronizing Standby control module is currently synchronizing• not-ready Standby control module is not synchronized
Configurable	False

resource-monitoring

Context	platform resource-monitoring
Tree	resource-monitoring
Description	
Configurable	True

acl

Context	platform resource-monitoring acl
Tree	acl
Description	
Configurable	True

resource *name identityref*

Context	platform resource-monitoring acl resource name identityref
Tree	resource
Description	
Configurable	True

name *identityref*

Context	platform resource-monitoring acl resource name identityref
Description	The name of the ACL resource
Options	<ul style="list-style-type: none">input-ipv4-filter-instances An input-ipv4-filter-instance resource is used every time an IPv4 filter instance is created and applied to ingress traffic on the forwarding complex. Only one instance is used if the subinterface-specific property of the filter is set to output-only; otherwise one instance is used for every subinterface using the IPv4 filter.input-ipv6-filter-instances An input-ipv6-filter-instance resource is used every time an IPv6 filter instance is created and applied to ingress traffic on the forwarding complex. Only one instance is used if the subinterface-specific property of the filter is set to output-only; otherwise one instance is used for every subinterface using the IPv6 filter.
Configurable	True

falling-threshold-log *number*

Context	platform resource-monitoring acl resource name <i>identityref</i> falling-threshold-log number
Tree	falling-threshold-log
Description	Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the ACL resource in any linecard/complex/core falls reaches this value in a falling direction
Range	0 to 100
Default	70
Configurable	True

rising-threshold-log *number*

Context	platform resource-monitoring acl resource name <i>identityref</i> rising-threshold-log number
Tree	rising-threshold-log
Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the ACL resource in any linecard/complex/core reaches this value in a rising direction
Range	0 to 100
Default	90
Configurable	True

ip-mpls-forwarding

Context	platform resource-monitoring ip-mpls-forwarding
Tree	ip-mpls-forwarding
Description	
Configurable	True

resource name *identityref*

Context	platform resource-monitoring ip-mpls-forwarding resource name <i>identityref</i>
Tree	resource
Description	
Configurable	True

name *identityref*

Context	platform resource-monitoring ip-mpls-forwarding resource name <i>identityref</i>
Description	The name of the IP-MPLS forwarding resource
Options	<ul style="list-style-type: none"> • ip-fib Each IP route (ECMP or non-ECMP) to an IPv4 or IPv6 prefix uses one of these resources. The underlying resource in J2 is the KAPS1 table. • ip-arp-nd Each IPv4 ARP entry and each IPv6 neighbor entry uses one of these resources. • direct-next-hops Each direct next-hop in a next-hop-group (static or dynamic) uses one of these resources. A direct next-hop is resolved by a local interface route. The same direct next-hop in two different NHGs still counts as one direct next-hop. • indirect-next-hops Each indirect next-hop in a next-hop-group (static or dynamic) uses one of these resources. An indirect next-hop is resolved by any route other than a local interface route. The same indirect next-hop in two different NHGs still counts as one indirect next-hop. • hardware-ecmp-fecs This represents the pool of resources used to support ECMP forwarding in hardware. On a J2 IMM the utilization for this pool of resources is calculated as the maximum utilization of the following tables: L1 ECMP FECs, L2 ECMP FECs, L1 ECMP member FECs and L2 ECMP member FECs • hardware-fecs This represents the pool of resources used to support non-ECMP forwarding in hardware. On a J2 IMM the utilization for this pool of resources is calculated as the maximum utilization of the following tables: L1 non-ECMP FECs, L2 non-ECMP FECs.
Configurable	True

falling-threshold-log *number*

Context	platform resource-monitoring ip-mpls-forwarding resource name <i>identityref</i> falling-threshold-log <i>number</i>
Tree	falling-threshold-log
Description	Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the IP-MPLS forwarding resource in any linecard/complex/core reaches this value in a falling direction
Range	0 to 100
Default	70
Configurable	True

rising-threshold-log *number*

Context	platform resource-monitoring ip-mpls-forwarding resource name <i>identityref</i> rising-threshold-log <i>number</i>
Tree	rising-threshold-log
Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the IP-MPLS forwarding resource in any linecard/complex/core reaches this value in a rising direction
Range	0 to 100
Default	90
Configurable	True

mtu

Context	platform resource-monitoring mtu
Tree	mtu
Description	
Configurable	True

resource name *identityref*

Context	platform resource-monitoring mtu resource name <i>identityref</i>
Tree	resource
Description	
Configurable	True

name *identityref*

Context	platform resource-monitoring mtu resource name <i>identityref</i>
Description	The name of the MTU resource
Options	<ul style="list-style-type: none">ip-mtu IP MTU resource pool. One resource from this pool is consumed by every different IP MTU value used by the subinterfaces on the linecard forwarding-complex.port-mtu Port MTU resource pool. One resource from this pool is consumed by every different port MTU value used by a port on the linecard forwarding-complex.
Configurable	True

falling-threshold-log *number*

Context	platform resource-monitoring mtu resource name <i>identityref</i> falling-threshold-log number
Tree	falling-threshold-log
Description	Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the MTU resource in any linecard/complex/core reaches this value in a falling direction and this is the first trigger since the last rising-threshold-log was triggered.
Range	0 to 100
Default	70
Configurable	True

rising-threshold-log *number*

Context	platform resource-monitoring mtu resource name <i>identityref</i> rising-threshold-log number
Tree	rising-threshold-log
Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the MTU resource in any linecard/complex/core reaches this value in a rising direction and this is the first trigger since the last restart or since the last falling-threshold-log was triggered.
Range	0 to 100
Default	90
Configurable	True

qos

Context	platform resource-monitoring qos
Tree	qos
Description	
Configurable	True

resource name *identityref*

Context	platform resource-monitoring qos resource name <i>identityref</i>
Tree	resource
Description	
Configurable	True

name *identityref*

Context	platform resource-monitoring qos resource name <i>identityref</i>
Description	The name of the QoS resource
Options	<ul style="list-style-type: none">• classifier-profiles A classifier-profile resource is used every time a different combination of DSCP classifier and MPLS-TC classifier is applied to an ingress subinterface of the forwarding complex. There are 16 of these resources and one is always used by the combination of the default DSCP classifier and the default MPLS TC classifier.• rewrite-profiles A rewrite-profile resource is used every time a different combination of DSCP rewrite-rule and MPLS-TC rewrite-rule is applied to an egress subinterface of the forwarding complex. There are 32 of these resources.
Configurable	True

falling-threshold-log *number*

Context	platform resource-monitoring qos resource name <i>identityref</i> falling-threshold-log <i>number</i>
Tree	falling-threshold-log
Description	Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the QoS resource in any linecard/complex/core falls reaches this value in a falling direction
Range	0 to 100
Default	70
Configurable	True

rising-threshold-log *number*

Context	platform resource-monitoring qos resource name <i>identityref</i> rising-threshold-log <i>number</i>
Tree	rising-threshold-log
Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the QoS resource in any linecard/complex/core reaches this value in a rising direction
Range	0 to 100
Default	90
Configurable	True

tcam

Context	platform resource-monitoring tcam
Tree	tcam
Description	
Configurable	True

resource [name](#) *identityref*

Context	platform resource-monitoring tcam resource name <i>identityref</i>
Tree	resource
Description	
Configurable	True

[name](#) *identityref*

Context	platform resource-monitoring tcam resource name <i>identityref</i>
Description	The name of the TCAM resource
Options	<ul style="list-style-type: none">• if-input-ipv4 Resource pool of TCAM entries used by IPv4 ACLs applied as subinterface-input filers• if-output-ipv4 Resource pool of TCAM entries used by IPv4 ACLs applied as subinterface-output filers• if-input-ipv6 Resource pool of TCAM entries used by IPv6 ACLs applied as subinterface-input filers• if-output-ipv6 Resource pool of TCAM entries used by IPv6 ACLs applied as subinterface-output filers• cpm-capture-ipv4 Resource pool of TCAM entries used by IPv4 cpm-filter ACLs and capture-filter ACLs• cpm-capture-ipv6 Resource pool of TCAM entries used by IPv6 cpm-filter ACLs and capture-filter ACLs
Configurable	True

falling-threshold-log *number*

Context	platform resource-monitoring tcam resource name <i>identityref</i> falling-threshold-log number
Tree	falling-threshold-log
Description	Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the TCAM resource in any linecard/complex/core falls reaches this value in a falling direction
Range	0 to 100
Default	70
Configurable	True

rising-threshold-log *number*

Context	platform resource-monitoring tcam resource name <i>identityref</i> rising-threshold-log number
Tree	rising-threshold-log
Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the TCAM resource in any linecard/complex/core reaches this value in a rising direction
Range	0 to 100
Default	90
Configurable	True

7 qos

qos

- + **classifiers**
 - + **dscp-policy name** *string*
 - + **dscp value** *number*
 - + **forwarding-class** *keyword*
 - + **mpls-traffic-class-policy name** *string*
 - + **traffic-class value** *number*
 - + **forwarding-class** *keyword*
- + **rewrite-rules**
 - + **dscp-policy name** *string*
 - + **map forwarding-class** *keyword*
 - + **dscp** (*number* | *keyword*)
 - + **mpls-traffic-class-policy name** *string*
 - + **map forwarding-class** *keyword*
 - + **traffic-class** *number*

7.1 qos Descriptions

qos

Context	qos
Tree	qos
Description	Top-level container for QoS data
Configurable	True

classifiers

Context	qos classifiers
Tree	classifiers
Description	QoS classifier
Configurable	True

dscp-policy *name string*

Context	qos classifiers dscp-policy name string
Tree	dscp-policy
Description	DSCP classification policy
Configurable	True

name *string*

Context	qos classifiers dscp-policy name string
Description	User-configured name for a DSCP classification policy The name 'default' is reserved for the system default DSCP classifier.
String Length	1 to 255
Configurable	True

dscp *value number*

Context	qos classifiers dscp-policy name string dscp value number
Tree	dscp
Description	DSCP codepoint
Configurable	True

value *number*

Context	qos classifiers dscp-policy name <i>string</i> dscp value <i>number</i>
Description	DSCP codepoint value, expressed as a number in the range 0-63
Range	0 to 63
Configurable	True

forwarding-class *keyword*

Context	qos classifiers dscp-policy name <i>string</i> dscp value <i>number</i> forwarding-class <i>keyword</i>
Tree	forwarding-class
Description	The forwarding class to which the DSCP value is mapped
Options	<ul style="list-style-type: none">• fc0• fc1• fc2• fc3• fc4• fc5• fc6• fc7
Configurable	True

mpls-traffic-class-policy [name](#) *string*

Context	qos classifiers mpls-traffic-class-policy name <i>string</i>
Tree	mpls-traffic-class-policy
Description	
Configurable	True

name *string*

Context	qos classifiers mpls-traffic-class-policy name <i>string</i>
Description	User-configured name for an MPLS traffic-class classification policy The name 'default' is reserved for the system default MPLS TC classifier.
String Length	1 to 255
Configurable	True

traffic-class value *number*

Context	qos classifiers mpls-traffic-class-policy name <i>string</i> traffic-class value <i>number</i>
Tree	traffic-class
Description	Traffic class container
Configurable	True

value *number*

Context	qos classifiers mpls-traffic-class-policy name <i>string</i> traffic-class value <i>number</i>
Description	A single traffic-class value
Range	0 to 7
Configurable	True

forwarding-class *keyword*

Context	qos classifiers mpls-traffic-class-policy name <i>string</i> traffic-class value <i>number</i> forwarding-class <i>keyword</i>
Tree	forwarding-class
Description	The forwarding class to which the traffic-class value is mapped
Options	<ul style="list-style-type: none">• fc0• fc1• fc2• fc3• fc4• fc5• fc6• fc7
Configurable	True

rewrite-rules

Context	qos rewrite-rules
Tree	rewrite-rules
Description	
Configurable	True

dscp-policy name *string*

Context	qos rewrite-rules dscp-policy name <i>string</i>
Tree	dscp-policy
Description	DSCP rewrite policy
Configurable	True

name *string*

Context	qos rewrite-rules dscp-policy name <i>string</i>
Description	User-configured name for a DSCP rewrite policy.
String Length	1 to 255
Configurable	True

map forwarding-class *keyword*

Context	qos rewrite-rules dscp-policy name <i>string</i> map forwarding-class <i>keyword</i>
Tree	map
Description	
Configurable	True

forwarding-class *keyword*

Context	qos rewrite-rules dscp-policy name <i>string</i> map forwarding-class <i>keyword</i>
Description	The forwarding-class value
Options	<ul style="list-style-type: none">• fc0• fc1• fc2• fc3• fc4• fc5• fc6• fc7
Configurable	True

dscp (*number | keyword*)

Context	qos rewrite-rules dscp-policy name <i>string map forwarding-class keyword dscp (number keyword)</i>
Tree	dscp
Description	DSCP value
Range	0 to 63
Options	<ul style="list-style-type: none">• CS0• LE• CS1• AF11• AF12• AF13• CS2• AF21• AF22• AF23• CS3• AF31• AF32• AF33• CS4• AF41• AF42• AF43• CS5• EF• CS6• CS7
Configurable	True

mpls-traffic-class-policy **name** *string*

Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i>
Tree	mpls-traffic-class-policy
Description	
Configurable	True

name *string*

Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i>
Description	User-configured name for an MPLS traffic-class rewrite policy.
String Length	1 to 255
Configurable	True

map forwarding-class *keyword*

Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i> map forwarding-class <i>keyword</i>
Tree	map
Description	
Configurable	True

forwarding-class *keyword*

Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i> map forwarding-class <i>keyword</i>
Description	The forwarding-class value
Options	<ul style="list-style-type: none">• fc0• fc1• fc2• fc3• fc4• fc5• fc6• fc7
Configurable	True

traffic-class *number*

Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i> map forwarding-class <i>keyword</i> traffic-class <i>number</i>
Tree	traffic-class
Description	The MPLS traffic class value to mark the packet with
Range	0 to 7
Configurable	True

8 routing-policy

routing-policy

- + **as-path-set name** *string*
 - + **expression** *string*
- + **community-set name** *string*
 - + **member** (*bgp-std-community-type | bgp-std-community-regexp-type | identityref | bgp-large-community-type | bgp-large-community-regexp-type*)
- + **policy name** *string*
 - + **default-action**
 - + **accept**
 - + **bgp**
 - + **as-path**
 - + **prepend**
 - + **as-number** (*number | keyword*)
 - + **repeat-n** *number*
 - + **replace** *string*
 - + **communities**
 - + **add** *reference*
 - + **remove** *reference*
 - + **replace** *reference*
 - + **local-preference**
 - + **set** *number*
 - + **origin**
 - + **set** *keyword*
 - + **next-entry**
 - + **next-policy**
 - + **reject**
 - + **statement sequence-id** *number*
 - + **action**
 - + **accept**
 - + **bgp**
 - + **as-path**
 - + **prepend**
 - + **as-number** (*number | keyword*)
 - + **repeat-n** *number*
 - + **replace** *string*
 - + **communities**
 - + **add** *reference*
 - + **remove** *reference*
 - + **replace** *reference*
 - + **local-preference**
 - + **set** *number*
 - + **origin**
 - + **set** *keyword*
 - + **next-entry**
 - + **next-policy**
 - + **reject**
 - + **match**
 - + **bgp**
 - + **as-path-length**
 - + **operator** *keyword*

- + **unique** *boolean*
- + **value** *number*
- + **as-path-set** *reference*
- + **community-set** *reference*
- + **family** *keyword*
- + **prefix-set** *reference*
- + **protocol** *identityref*
- + **prefix-set name** *string*
 - + **prefix ip-prefix** (*ipv4-prefix | ipv6-prefix*) **mask-length-range** *string*

8.1 routing-policy Descriptions

routing-policy

Context	routing-policy
Tree	routing-policy
Description	Top-level container for all routing policy configuration
Configurable	True

as-path-set **name** *string*

Context	routing-policy as-path-set name <i>string</i>
Tree	as-path-set
Description	AS Path regular expressions for use in policy entries
Configurable	True

name *string*

Context	routing-policy as-path-set name <i>string</i>
Description	A name used to identify the AS path regular expression
String Length	1 to 255
Configurable	True

expression *string*

Context	routing-policy as-path-set name <i>string</i> expression <i>string</i>
Tree	expression
Description	A regular expression where each AS number is an elemental term
String Length	1 to 65535
Configurable	True

community-set **name** *string*

Context	routing-policy community-set name <i>string</i>
Tree	community-set
Description	List of BGP community sets containing standard and large BGP communities
Configurable	True

name *string*

Context	routing-policy community-set name <i>string</i>
Description	A name used to identify the community set
String Length	1 to 255
Configurable	True

member (*bgp-std-community-type | bgp-std-community-regexp-type | identityref | bgp-large-community-type | bgp-large-community-regexp-type*)

Context	routing-policy community-set name <i>string</i> member (<i>bgp-std-community-type bgp-std-community-regexp-type identityref bgp-large-community-type bgp-large-community-regexp-type</i>)
Tree	member
Description	A standard BGP community value, regular expression or well-known name or else a large BGP community value or regular expression
Options	<ul style="list-style-type: none">• no-export Do not export NLRI received carrying this community outside the bounds of this autonomous system, or this confederation if the local autonomous system is a confederation member AS. This community has a value of 0xFFFFFFFF01.• no-advertise All NLRI received carrying this community must not be advertised to other BGP peers. This community has a value of 0xFFFFFFFF02.• no-export-subconfed All NLRI received carrying this community must not be advertised to external BGP peers - including over confederation sub-AS boundaries. This community has a value of 0xFFFFFFFF03.
Configurable	True
Min. Elements	1

policy name *string*

Context	routing-policy policy name <i>string</i>
Tree	policy
Description	List of policy definitions, keyed by unique name These policy definitions are expected to be referenced (by name) in policy in import-policy and/or export-policy statements.
Configurable	True

name *string*

Context	routing-policy policy name <i>string</i>
Description	A name used to identify the policy
String Length	1 to 255
Configurable	True

default-action

Context	routing-policy policy name <i>string</i> default-action
Tree	default-action
Description	Actions for routes that do not match any policy entry
Configurable	True

accept

Context	routing-policy policy name <i>string</i> default-action accept
Tree	accept
Description	Accept action
Configurable	True

bgp

Context	routing-policy policy name <i>string</i> default-action accept bgp
Tree	bgp
Description	
Configurable	True

as-path

Context	routing-policy policy name <i>string</i> default-action accept bgp as-path
Tree	as-path
Description	Modify AS Path attribute of routes
Configurable	True

prepend

Context	routing-policy policy name <i>string</i> default-action accept bgp as-path prepend
Tree	prepend
Description	Prepend a BGP AS number to the AS Path attribute of routes
Configurable	True

as-number (*number | keyword*)

Context	routing-policy policy name <i>string</i> default-action accept bgp as-path prepend as-number (<i>number keyword</i>)
Tree	as-number
Description	The AS number to prepend to the AS Path attributes If 'auto' is specified then the peer's AS number is used in the context of an import policy and the local AS number is used in the context of an export policy.
Range	1 to 4294967295
Options	<ul style="list-style-type: none">• auto
Configurable	True

repeat-n *number*

Context	routing-policy policy name <i>string</i> default-action accept bgp as-path prepend repeat-n <i>number</i>
Tree	repeat-n
Description	The number of repetitions of the prepended AS number
Range	1 to 50
Default	1
Configurable	True

replace *string*

Context	routing-policy policy name <i>string</i> default-action accept bgp as-path replace <i>string</i>
Tree	replace
Description	Replace as-path
Configurable	True

communities

Context	routing-policy policy name <i>string</i> default-action accept bgp communities
Tree	communities
Description	Modify BGP communities attached to routes
Configurable	True

add *reference*

Context	routing-policy policy name <i>string</i> default-action accept bgp communities add <i>reference</i>
Tree	add
Description	Reference to a community-set name All of the non-regex community members in the referenced community-set are added to the COMMUNITIES and LARGE_COMMUNITIES attributes.
Reference	routing-policy community-set name <i>string</i>
Configurable	True

remove *reference*

Context	routing-policy policy name <i>string</i> default-action accept bgp communities remove <i>reference</i>
Tree	remove
Description	Reference to a community-set name The communities in the route are compared to all of the community members in the referenced community-set, and all matching communities are removed from the COMMUNITIES and LARGE_COMMUNITIES attributes.
Reference	routing-policy community-set name <i>string</i>
Configurable	True

replace *reference*

Context	routing-policy policy name <i>string</i> default-action accept bgp communities replace <i>reference</i>
Tree	replace
Description	Reference to a community-set name

All of the existing communities are deleted and then all of the non-regex community members in the referenced community-set are encoded in new COMMUNITIES and LARGE_COMMUNITIES attributes.

Reference **routing-policy community-set name** *string*
Configurable True

local-preference

Context **routing-policy policy name** *string* **default-action accept bgp local-preference**
Tree **local-preference**
Description
Configurable True

set number

Context **routing-policy policy name** *string* **default-action accept bgp local-preference set number**
Tree **set**
Description The new value of LOCAL_PREF to write into the matching BGP routes
Configurable True

origin

Context **routing-policy policy name** *string* **default-action accept bgp origin**
Tree **origin**
Description
Configurable True

set keyword

Context **routing-policy policy name** *string* **default-action accept bgp origin set keyword**
Tree **set**
Description The new value of the ORIGIN attribute to write into the matching BGP routes
Options

- igp
- egp
- incomplete

Configurable True

next-entry

Context	routing-policy policy name <i>string</i> default-action next-entry
Tree	next-entry
Description	Next entry action
Configurable	True

next-policy

Context	routing-policy policy name <i>string</i> default-action next-policy
Tree	next-policy
Description	Next policy action
Configurable	True

reject

Context	routing-policy policy name <i>string</i> default-action reject
Tree	reject
Description	Reject action
Configurable	True

statement [sequence-id](#) *number*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i>
Tree	statement
Description	Policy statements group conditions and actions within a policy definition. They are evaluated in the order of their sequence id.
Configurable	True

[sequence-id](#) *number*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i>
Description	Number indicating when this policy statement should be evaluated relative to other policy statements Lower numbered statements are evaluated before higher numbered statements.
Range	1 to 4294967295
Configurable	True

action

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action
Tree	action
Description	Policy actions
Configurable	True

accept

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept
Tree	accept
Description	Accept action
Configurable	True

bgp

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp
Tree	bgp
Description	BGP specific action
Configurable	True

as-path

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path
Tree	as-path
Description	Modify AS Path attribute of routes
Configurable	True

prepend

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path prepend
Tree	prepend
Description	Prepend a BGP AS number to the AS Path attribute of routes
Configurable	True

as-number (*number | keyword*)

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path prepend as-number (<i>number keyword</i>)
Tree	as-number
Description	The AS number to prepend to the AS Path attributes If 'auto' is specified then the peer's AS number is used in the context of an import policy and the local AS number is used in the context of an export policy.
Range	1 to 4294967295
Options	<ul style="list-style-type: none">• auto
Configurable	True

repeat-n *number*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path prepend repeat-n <i>number</i>
Tree	repeat-n
Description	The number of repetitions of the prepended AS number
Range	1 to 50
Default	1
Configurable	True

replace *string*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path replace <i>string</i>
Tree	replace
Description	Replace as-path
Configurable	True

communities

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities
Tree	communities
Description	Modify BGP communities attached to routes
Configurable	True

add *reference*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities add <i>reference</i>
Tree	add
Description	Reference to a community-set name All of the non-regex community members in the referenced community-set are added to the COMMUNITIES and LARGE_COMMUNITIES attributes.
Reference	routing-policy community-set name <i>string</i>
Configurable	True

remove *reference*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities remove <i>reference</i>
Tree	remove
Description	Reference to a community-set name The communities in the route are compared to all of the community members in the referenced community-set, and all matching communities are removed from the COMMUNITIES and LARGE_COMMUNITIES attributes.
Reference	routing-policy community-set name <i>string</i>
Configurable	True

replace *reference*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities replace <i>reference</i>
Tree	replace
Description	Reference to a community-set name All of the existing communities are deleted and then all of the non-regex community members in the referenced community-set are encoded in new COMMUNITIES and LARGE_COMMUNITIES attributes.
Reference	routing-policy community-set name <i>string</i>
Configurable	True

local-preference

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp local-preference
Tree	local-preference
Description	LOCAL_PREF attribute
Configurable	True

set number

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp local-preference set <i>number</i>
Tree	set
Description	The new value of LOCAL_PREF to write into the matching BGP routes
Configurable	True

origin

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp origin
Tree	origin
Description	ORIGIN attribute
Configurable	True

set keyword

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp origin set <i>keyword</i>
Tree	set
Description	The new value of the ORIGIN attribute to write into the matching BGP routes
Options	<ul style="list-style-type: none">• <code>igp</code>• <code>egp</code>• <code>incomplete</code>
Configurable	True

next-entry

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action next-entry
Tree	next-entry
Description	next entry action
Configurable	True

next-policy

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action next-policy
Tree	next-policy
Description	next policy action
Configurable	True

reject

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action reject
Tree	reject
Description	Reject action
Configurable	True

match

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match
Tree	match
Description	Match conditions of the policy statement
Configurable	True

bgp

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp
Tree	bgp
Description	Top-level container
Configurable	True

as-path-length

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp as-path-length
Tree	as-path-length
Description	A BGP route matches this condition if the number of (unique) AS numbers in its AS_PATH matches this value or the range implied by the value+operator.
Configurable	True

operator *keyword*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp as-path-length operator <i>keyword</i>
Tree	operator
Description	The comparison operator that applies to the value
Default	eq
Options	<ul style="list-style-type: none">• eq• ge• le
Configurable	True

unique *boolean*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp as-path-length unique <i>boolean</i>
Tree	unique
Description	Count a repeated sequence of the same AS number as just 1 element
Default	false
Configurable	True

value *number*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp as-path-length value <i>number</i>
Tree	value
Description	The number of (unique) AS numbers in the AS path
Range	0 to 255
Configurable	True

as-path-set *reference*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp as-path-set <i>reference</i>
Tree	as-path-set
Description	Reference to an as-path-set name A route meets this condition if it matches the regular expression
Reference	routing-policy as-path-set name <i>string</i>
Configurable	True

community-set *reference*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp community-set <i>reference</i>
Tree	community-set
Description	Reference to a community-set name A route meets this condition if has any community value matching a community member in the referenced community-set
Reference	routing-policy community-set name <i>string</i>
Configurable	True

family *keyword*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp family <i>keyword</i>
Tree	family
Description	The address families that this condition would match against
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	True

prefix-set *reference*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match prefix-set <i>reference</i>
Tree	prefix-set
Description	Reference to a prefix set name
Reference	routing-policy prefix-set name <i>string</i>
Configurable	True

protocol *identityref*

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match protocol <i>identityref</i>
Tree	protocol
Description	The protocol name or route owner name to match
Options	<ul style="list-style-type: none">• bgp Border Gateway Protocol version 4• isis IS-IS• ospfv2 OSPFv2• ospfv3 OSPFv3• static Locally configured static route• local A directly connected route• host A host route• aggregate Locally configured aggregate route• sdk IP route added by an agent application using the SDK• linux-mgr IP route added by the linux kernel.• dhcp-client-mgr IP route added by DHCP client
Configurable	True

prefix-set name *string*

Context	routing-policy prefix-set name <i>string</i>
Tree	prefix-set
Description	List of defined prefix sets
Configurable	True

name *string*

Context	routing-policy prefix-set name <i>string</i>
Description	A name used to identify the prefix set
String Length	1 to 255
Configurable	True

prefix ip-prefix (*ipv4-prefix | ipv6-prefix*) **mask-length-range** *string*

Context	routing-policy prefix-set name <i>string</i> prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>) mask-length-range <i>string</i>
Tree	prefix
Description	List of prefixes in the prefix set
Configurable	True

ip-prefix (*ipv4-prefix | ipv6-prefix*)

Context	routing-policy prefix-set name <i>string</i> prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>) mask-length-range <i>string</i>
Description	The IPv4 or IPv6 prefix in CIDR notation
Configurable	True

mask-length-range *string*

Context	routing-policy prefix-set name <i>string</i> prefix ip-prefix (<i>ipv4-prefix ipv6-prefix</i>) mask-length-range <i>string</i>
Description	The range of prefix lengths to match Example: 10.3.192.0/21 through 10.3.192.0/24 would be expressed as prefix: 10.3.192.0/21, mask-length-range: 21..24. Example: 10.3.192.0/21 would be expressed as prefix: 10.3.192.0/21, mask-length-range: exact
Configurable	True

9 system

system

- + **aaa**
 - + **accounting**
 - + **accounting-method** *reference*
 - + **event event-type** *identityref*
 - + **record** *identityref*
 - + **authentication**
 - + **admin-user**
 - + **password** *string*
 - **username** *string*
 - + **authentication-method** *reference*
 - + **exit-on-reject** *boolean*
 - + **idle-timeout** *number*
 - **session id** *number*
 - **login-time** *string*
 - **remote-host** *string*
 - **service-name** *string*
 - **tty-name** *string*
 - **username** *string*
 - + **server-group name** *string*
 - + **server address** (*ipv4-address | ipv6-address*)
 - + **name** *string*
 - + **network-instance** *reference*
 - **oper-state** *keyword*
 - **statistics**
 - **accounting-connection-failures** *number*
 - **accounting-rejects** *number*
 - **accounting-success** *number*
 - **login-connection-failures** *number*
 - **login-rejects** *number*
 - **login-success** *number*
 - + **tacacs**
 - + **port** *number*
 - + **secret-key** *string*
 - + **timeout** *number*
 - + **type** *identityref*
 - **app-management**
 - **application name** *string*
 - **author** *string*
 - **failure-action** *string*
 - **failure-threshold** *number*
 - **failure-window** *number*
 - **last-change** *string*
 - **launch-command** *string*
 - **path** *string*
 - **pid** *number*
 - **restricted-operations** *keyword*
 - **search-command** *string*
 - **state** *keyword*
 - **statistics**

- **restart-count** *number*
- **version** *string*
- **yang**
 - **modules** *string*
 - **source-directories** *string*
- + **authentication**
 - + **keychain name** *string*
 - + **admin-state** *keyword*
 - + **description** *string*
 - + **key index** *number*
 - + **algorithm** *keyword*
 - + **authentication-key** *string*
 - + **type** *keyword*
- + **banner**
 - + **login-banner** *string*
 - + **motd-banner** *string*
- + **boot**
 - + **autoboot**
 - + **admin-state** *keyword*
 - + **attempts** *number*
 - + **client-id** *keyword*
 - + **interface** *reference*
 - **oper-state** *string*
 - + **timeout** *number*
 - + **image** *string*
- + **clock**
 - + **timezone** *keyword*
- + **configuration**
 - **candidate name** *string*
 - **started** *string*
 - **type** *keyword*
 - **username** *string*
 - **checkpoint id** *number*
 - **comment** *string*
 - **created** *string*
 - **name** *string*
 - **size** *number*
 - **username** *string*
 - **version** *string*
 - **commit id** *number*
 - **comment** *string*
 - **ended** *string*
 - **name** *string*
 - **started** *string*
 - **status** *keyword*
 - **type** *keyword*
 - **username** *string*
 - + **idle-timeout** *number*
 - **last-change** *string*
 - + **max-candidates** *number*
 - + **max-checkpoints** *number*
 - **session id** *number*
 - **exclusive** *boolean*
 - **name** *string*

- **started** *string*
- **type** *keyword*
- **username** *string*
- + **dns**
 - + **host-entry name** *string*
 - + **ipv4-address** *string*
 - + **ipv6-address** *string*
 - + **network-instance** *reference*
 - **oper-state** *keyword*
 - + **search-list** *string*
 - + **server-list** (*ipv4-address | ipv6-address*)
- **features** *string*
- + **ftp-server**
 - + **network-instance name** *reference*
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - + **session-limit** *number*
 - + **source-address** (*ipv4-address | ipv6-address*)
 - + **timeout** *number*
- + **gnmi-server**
 - + **admin-state** *keyword*
 - + **commit-confirmed-timeout** *number*
 - + **network-instance name** *reference*
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - + **port** *number*
 - + **source-address** (*ipv4-address | ipv6-address*)
 - + **tls-profile** *reference*
 - + **use-authentication** *boolean*
 - + **rate-limit** *number*
 - + **session-limit** *number*
 - **subscription id** *number*
 - **mode** *keyword*
 - **paths** *string*
 - **remote-host** (*ipv4-address | ipv6-address*)
 - **remote-port** *number*
 - **sample-interval** *number*
 - **start-time** *string*
 - **user** *string*
 - **user-agent** *string*
 - + **timeout** *number*
 - + **trace-options** *keyword*
 - + **unix-socket**
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - **socket-path** *string*
 - + **tls-profile** *reference*
 - + **use-authentication** *boolean*
- + **information**
 - + **contact** *string*
 - **current-datetime** *string*
 - **description** *string*
 - + **location** *string*
 - **uptime** *string*

- **version** *string*
- + **ip-load-balancing**
 - + **hash-keys**
 - + **hash-seed** *number*
- + **json-rpc-server**
 - + **admin-state** *keyword*
 - + **commit-confirmed-timeout** *number*
 - + **network-instance name** *reference*
 - + **http**
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - + **port** *number*
 - + **session-limit** *number*
 - + **source-address** (*ipv4-address | ipv6-address*)
 - + **use-authentication** *boolean*
 - + **https**
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - + **port** *number*
 - + **session-limit** *number*
 - + **source-address** (*ipv4-address | ipv6-address*)
 - + **tls-profile** *reference*
 - + **use-authentication** *boolean*
 - + **trace-options** *keyword*
 - + **unix-socket**
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - **socket-path** *string*
 - + **tls-profile** *reference*
 - + **use-authentication** *boolean*
- + **lACP**
 - + **system-id** *string*
 - + **system-priority** *number*
- + **lldp**
 - + **admin-state** *keyword*
 - + **bgp-auto-discovery**
 - + **admin-state** *keyword*
 - + **group-id** *number*
 - + **network-instance** *reference*
 - **chassis-id** *string*
 - **chassis-id-type** *keyword*
 - + **hello-timer** *number*
 - + **hold-multiplier** *number*
 - + **interface name** *reference*
 - + **admin-state** *keyword*
 - + **bgp-auto-discovery**
 - + **admin-state** *keyword*
 - + **group-id** *number*
 - + **peering-address** (*ipv4-address | ipv6-address*)
 - **neighbor id** *string*
 - **bgp-auto-discovery**
 - **bgp-peer-addresses** *string*
 - **group-id** *number*
 - **capability name** *string*

- **enabled** *boolean*
- **chassis-id** *string*
- **chassis-id-type** *keyword*
- **custom-tlv type** *number* **oui** *string* **oui-subtype** *string*
 - **value** *binary*
- **first-message** *string*
- **last-update** *string*
- **management-address address** *string*
 - **type** *keyword*
- **port-description** *string*
- **port-id** (*string* | *binary*)
- **port-id-type** *keyword*
- **system-description** *string*
- **system-name** *string*
- **oper-state** *keyword*
- **statistics**
 - **frame-discard** *number*
 - **frame-error-in** *number*
 - **frame-error-out** *number*
 - **frame-in** *number*
 - **frame-out** *number*
 - **last-clear** *string*
 - **tlv-discard** *number*
 - **tlv-unknown** *number*
- + **management-address subinterface** *string*
 - + **type** *keyword*
- **statistics**
 - **entries-aged-out** *number*
 - **frame-discard** *number*
 - **frame-error-in** *number*
 - **frame-in** *number*
 - **frame-out** *number*
 - **last-clear** *string*
 - **tlv-accepted** *number*
 - **tlv-discard** *number*
 - **tlv-unknown** *number*
- **system-description** *string*
- **system-name** *string*
- + **trace-options** *keyword*
- + **logging**
 - + **buffer buffer-name** *string*
 - + **facility facility-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
 - + **filter** *reference*
 - + **format** *string*
 - + **persist** *number*
 - + **rotate** *number*
 - **rotations** *number*
 - + **size** *string*
 - + **subsystem subsystem-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*

- +
 - + **match-exact** *keyword*
- + **console**
 - + **facility** **facility-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
 - + **filter** *reference*
 - + **format** *string*
 - + **subsystem** **subsystem-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
- + **file** **file-name** *string*
 - + **directory** *string*
 - + **facility** **facility-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
 - + **filter** *reference*
 - + **format** *string*
 - + **rotate** *number*
 - **rotations** *number*
 - + **size** *string*
 - + **subsystem** **subsystem-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
- + **filter** **filter-name** *string*
 - + **contains** *string*
 - + **facility** **facility-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
 - + **prefix** *string*
 - + **regex** *string*
 - + **tag** *string*
- + **network-instance** *reference*
- + **remote-server** **host** (*ipv4-address | ipv6-address | domain-name*)
 - + **facility** **facility-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
 - + **filter** *reference*
 - + **remote-port** *number*
 - + **subsystem** **subsystem-name** *keyword*
 - + **priority**
 - + **match-above** *keyword*
 - + **match-exact** *keyword*
 - + **transport** *keyword*
- + **subsystem-facility** *keyword*
- + **maintenance**
 - + **group name** *string*
 - + **maintenance-mode**
 - + **admin-state** *keyword*

- + **maintenance-profile** *reference*
- + **members**
 - + **bgp**
 - + **network-instance name** *reference*
 - + **neighbor** *reference*
 - + **peer-group** *reference*
- + **profile name** *string*
- + **bgp**
 - + **export-policy** *reference*
 - + **import-policy** *reference*
- + **mtu**
 - + **default-ip-mtu** *number*
 - + **default-l2-mtu** *number*
 - + **default-port-mtu** *number*
 - + **min-path-mtu** *number*
- + **name**
 - + **domain-name** *string*
 - + **host-name** *string*
- + **ntp**
 - + **admin-state** *keyword*
 - + **network-instance** *reference*
 - **oper-state** *keyword*
 - + **server address** (*ipv4-address | ipv6-address*)
 - + **iburst** *boolean*
 - **jitter** *string*
 - **offset** *string*
 - **poll-interval** *number*
 - + **prefer** *boolean*
 - **stratum** *number*
 - **synchronized** (*ipv4-address | ipv6-address | string*)
- + **sflow**
 - + **admin-state** *keyword*
 - + **collector collector-id** *number*
 - + **collector-address** (*ipv4-address | ipv6-address*)
 - + **network-instance** *reference*
 - **next-hop** (*ipv4-address | ipv6-address*)
 - + **port** *number*
 - + **source-address** (*ipv4-address | ipv6-address*)
 - + **sample-rate** *number*
 - + **sample-size** *number*
 - **statistics**
 - **total-offered-packets** *number*
 - **total-samples-taken** *number*
 - **total-sent-packets** *number*
- + **snmp**
 - + **community** *string*
 - + **network-instance name** *reference*
 - + **admin-state** *keyword*
 - **oper-state** *keyword*
 - + **source-address** (*ipv4-address | ipv6-address*)
- + **ssh-server**
 - + **network-instance name** *reference*
 - + **admin-state** *keyword*
 - **oper-state** *keyword*

-
- **protocol-version** *number*
 - + **rate-limit** *number*
 - + **source-address** (*ipv4-address | ipv6-address*)
 - + **timeout** *number*
 - + **tls**
 - + **server-profile name** *string*
 - + **authenticate-client** *boolean*
 - + **certificate** *string*
 - + **cipher-list** *identityref*
 - + **key** *string*
 - + **trust-anchor** *string*
 - + **trace-options** *keyword*

9.1 system Descriptions

system

Context	system
Tree	system
Description	Enclosing container for system management
Configurable	True

aaa

Context	system aaa
Tree	aaa
Description	Top-level container for AAA services
Configurable	True

accounting

Context	system aaa accounting
Tree	accounting
Description	Top-level container for accounting
Configurable	True

accounting-method *reference*

Context	system aaa accounting accounting-method <i>reference</i>
Tree	accounting-method
Description	Ordered list of server-groups to use for accounting in the system If accounting fails with one method, the next defined method is tried -- failure of all methods results in the accounting request failing.
Reference	system aaa server-group name <i>string</i>
Configurable	True

event *event-type identityref*

Context	system aaa accounting event event-type identityref
Tree	event
Description	List of events subject to accounting
Configurable	True

event-type *identityref*

Context	system aaa accounting event event-type identityref
Description	The type of activity to record at the accounting server
Options	<ul style="list-style-type: none">• command Specifies interactive command events for AAA accounting
Configurable	True

record *identityref*

Context	system aaa accounting event event-type identityref record identityref
Tree	record
Description	Type of record to send to the accounting server for this activity type
Options	<ul style="list-style-type: none">• start-stop Send start and stop records for user activities A start record is sent to the accounting server at the beginning of the activity, and a stop record at the end of the activity• stop Send only stop records for user activities A stop record is sent to the accounting server when the user activity completes
Configurable	True

authentication

Context	system aaa authentication
Tree	authentication
Description	Top-level container for global authentication data
Configurable	True

admin-user

Context	system aaa authentication admin-user
Tree	admin-user
Description	Enclosing container for admin user
Configurable	True

password *string*

Context	system aaa authentication admin-user password <i>string</i>
Tree	password
Description	The admin password, supplied as cleartext The system will hash the value, storing only the hashed value
Configurable	True

username *string*

Context	system aaa authentication admin-user username <i>string</i>
Tree	username
Description	Assigned username for admin user
Default	admin
Configurable	False

authentication-method *reference*

Context	system aaa authentication authentication-method <i>reference</i>
Tree	authentication-method
Description	Ordered list of server-groups to be used during user authentication If authentication fails with one method, the next defined method is tried -- failure of all methods results in the user being denied access.
Reference	system aaa server-group name <i>string</i>
Configurable	True

exit-on-reject *boolean*

Context	system aaa authentication exit-on-reject <i>boolean</i>
Tree	exit-on-reject
Description	Enable/disable exit-on-reject behaviour for authentication attempts

With this behaviour enabled, when a reject is received from any server the system will not try further methods, and will reject the user authentication attempt. Default behaviour is to continue trying methods until one accepts the user, or the system runs out of methods to try.

Default false
Configurable True

idle-timeout *number*

Context **system aaa authentication idle-timeout** *number*
Tree **idle-timeout**
Description Set the idle timeout of all CLI sessions
After the timeout is reached, the session is disconnected from the system.
Default 600
Units seconds
Configurable True
Introduced 20.4.1

session id *number*

Context **system aaa authentication session id** *number*
Tree **session**
Description List of active sessions in the system
Configurable False

id *number*

Context **system aaa authentication session id** *number*
Description System generated session ID
Configurable False

login-time *string*

Context **system aaa authentication session id** *number* **login-time** *string*
Tree **login-time**
Description Time the user logged in
Configurable False

remote-host *string*

Context	system aaa authentication session id <i>number remote-host string</i>
Tree	remote-host
Description	Remote host of the session
Configurable	False

service-name *string*

Context	system aaa authentication session id <i>number service-name string</i>
Tree	service-name
Description	Service name that called login for the session
Configurable	False

tty-name *string*

Context	system aaa authentication session id <i>number tty-name string</i>
Tree	tty-name
Description	Terminal type
Configurable	False

username *string*

Context	system aaa authentication session id <i>number username string</i>
Tree	username
Description	Username linked to the session
Configurable	False

server-group **name** *string*

Context	system aaa server-group name <i>string</i>
Tree	server-group
Description	List of AAA server-groups in the system Each server group specifies a type, of which all servers must use. If using the 'local' type, then no servers may be specified.
Configurable	True
Max. Elements	2

name *string*

Context	system aaa server-group name <i>string</i>
Description	User defined name for the server group
String Length	1 to 255
Configurable	True

server address (*ipv4-address | ipv6-address*)

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>)
Tree	server
Description	List of AAA servers to use within this server-group Servers are tried in a round-robin fashion, with the first server always being tried if it is operationally available
Configurable	True
Max. Elements	5

address (*ipv4-address | ipv6-address*)

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>)
Description	Address used to reach the server
Configurable	True

name *string*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) name <i>string</i>
Tree	name
Description	User defined name assigned to the server
String Length	1 to 255
Configurable	True

network-instance *reference*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) network-instance <i>reference</i>
Tree	network-instance
Description	Reference to a configured network-instance used for reachability to the server

This network-instance must already exist in the system, and different servers within the same server-group may use different network-instances for connectivity.

Reference **network-instance name** *string*

Configurable True

oper-state *keyword*

Context **system aaa server-group name** *string* **server address** (*ipv4-address | ipv6-address*)
oper-state *keyword*

Tree **oper-state**

Description Details the operational state of the server

A server is defined as being down if it fails to respond before the timeout period, or if a path towards the server is not available.

- Options
- up
Component or process is operational
 - down
Component or process is not operational
 - empty
Component slot is empty
 - downloading
Component is downloading image into memory
 - booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing
Component is currently being synchronized
 - upgrading
Component is currently being upgraded

Configurable False

statistics

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics
Tree	statistics
Description	Enclosing container for server statistics
Configurable	False

accounting-connection-failures *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics accounting-connection-failures <i>number</i>
Tree	accounting-connection-failures
Description	Number of accounting connection failures
Default	0
Configurable	False

accounting-rejects *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics accounting-rejects <i>number</i>
Tree	accounting-rejects
Description	Number of accounting rejections
Default	0
Configurable	False

accounting-success *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics accounting-success <i>number</i>
Tree	accounting-success
Description	Number of accounting successes
Default	0
Configurable	False

login-connection-failures *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics login-connection-failures <i>number</i>
Tree	login-connection-failures
Description	Number of login connection failures
Default	0
Configurable	False

login-rejects *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics login-rejects <i>number</i>
Tree	login-rejects
Description	Number of login rejections
Default	0
Configurable	False

login-success *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) statistics login-success <i>number</i>
Tree	login-success
Description	Number of login successes
Default	0
Configurable	False

tacacs

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) tacacs
Tree	tacacs
Description	Top-level container for TACACS+ server data
Configurable	True

port *number*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) tacacs port <i>number</i>
Tree	port
Description	The port number on which to contact the TACACS+ server
Range	0 to 65535
Default	49
Configurable	True

secret-key *string*

Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address ipv6-address</i>) tacacs secret-key <i>string</i>
Tree	secret-key
Description	The unencrypted shared key used between the system and server
Configurable	True

timeout *number*

Context	system aaa server-group name <i>string</i> timeout <i>number</i>
Tree	timeout
Description	Set the timeout in seconds on responses from servers in this group
Range	1 to 3600
Default	10
Units	seconds
Configurable	True

type *identityref*

Context	system aaa server-group name <i>string</i> type <i>identityref</i>
Tree	type
Description	AAA server type -- all servers in the group must be of this type
Options	<ul style="list-style-type: none">• tacacs Specifies servers using the TACACS+ protocol Terminal Access Controller Access Control System (TACACS+)• local Specifies using Linux local methods

This type cannot be combined with a server address

Configurable True

app-management

Context [system app-management](#)

Tree [app-management](#)

Description Top-level container for application configuration and state

Configurable False

application name *string*

Context [system app-management application name](#) *string*

Tree [application](#)

Description List of all applications managed by the application manager

Configurable False

name *string*

Context [system app-management application name](#) *string*

Description Unique name of this application instance

Configurable False

author *string*

Context [system app-management application name](#) *string* [author](#) *string*

Tree [author](#)

Description The author of the application

Configurable False

failure-action *string*

Context [system app-management application name](#) *string* [failure-action](#) *string*

Tree [failure-action](#)

Description The action taken after 'failure-threshold' failures within 'failure-window'

This action can be to reboot the system, wait forever, or wait for a predefined number of seconds

Configurable False

failure-threshold *number*

Context	system app-management application name <i>string</i> failure-threshold <i>number</i>
Tree	failure-threshold
Description	How many restarts within 'failure-window' are required to trigger the failure action Setting this value to 0 will result in no action taking place on application restarts
Range	0 to 255
Configurable	False

failure-window *number*

Context	system app-management application name <i>string</i> failure-window <i>number</i>
Tree	failure-window
Description	Sliding window in seconds, over which to count restarts towards failure-threshold
Range	300 to 86400
Units	seconds
Configurable	False

last-change *string*

Context	system app-management application name <i>string</i> last-change <i>string</i>
Tree	last-change
Description	Date and time the application instance last changed state
Configurable	False

launch-command *string*

Context	system app-management application name <i>string</i> launch-command <i>string</i>
Tree	launch-command
Description	The command used to launch the application
Configurable	False

path *string*

Context	system app-management application name <i>string</i> path <i>string</i>
Tree	path
Description	The directory where the application can be found
Configurable	False

pid *number*

Context	system app-management application name <i>string</i> pid <i>number</i>
Tree	pid
Description	Process ID of this application instance
Configurable	False

restricted-operations *keyword*

Context	system app-management application name <i>string</i> restricted-operations <i>keyword</i>
Tree	restricted-operations
Description	The operations that may not be manually performed on this application
Options	<ul style="list-style-type: none">• restart This application may not be restarted manually• stop This application may not be stopped manually• start This application may not be started manually• reload This application may not be reloaded manually• quit This application may not be terminated manually• kill This application may not be terminated ungracefully manually
Configurable	False

search-command *string*

Context	system app-management application name <i>string</i> search-command <i>string</i>
Tree	search-command
Description	The command used to search for the applications liveness
Configurable	False

state *keyword*

Context	system app-management application name <i>string</i> state <i>keyword</i>
Tree	state
Description	Current state of this application instance
Options	<ul style="list-style-type: none">• running Application instance is running This is the normal, active state of an application• waiting-for-config Application instance is loaded, but has no configuration This state requires <code>wait-for-config true</code> within the applications YAML configuration. This results in the application being loaded into <code>app-mgr</code>, but not starting until the system receives configuration for it• error The application has not started successfully, or has failed This state can be caused by an application hitting the restart backoff, or an application failing to start following triggering a system reboot• starting The application has been asked to start All applications enter this state after initial execution, after which application manager will wait five seconds before checking their status. IDB connected applications may announce their state before this five second window has passed, resulting in them transitioning from this state faster than PID-monitored applications.• stopped The application is not running This state is most likely caused by an operator action
Configurable	False

statistics

Context	system app-management application name <i>string</i> statistics
Tree	statistics
Description	Top-level container for application statistics
Configurable	False

restart-count *number*

Context	system app-management application name <i>string</i> statistics restart-count <i>number</i>
Tree	restart-count
Description	The number of times this application instance has restarted
Default	0
Configurable	False

version *string*

Context	system app-management application name <i>string</i> version <i>string</i>
Tree	version
Description	The version of the application
Configurable	False

yang

Context	system app-management application name <i>string</i> yang
Tree	yang
Description	Top-level container for application state related to YANG
Configurable	False

modules *string*

Context	system app-management application name <i>string</i> yang modules <i>string</i>
Tree	modules
Description	YANG module names used by this application instance
Configurable	False

source-directories *string*

Context	system app-management application name <i>string</i> yang source-directories <i>string</i>
Tree	source-directories
Description	Source directories searched for YANG modules to load These directories are used to load modules indicated in the modules leaf, and any modules imported/included within them
Configurable	False

authentication

Context	system authentication
Tree	authentication
Description	Container for protocol authentication options available system wide
Configurable	True

keychain name *string*

Context	system authentication keychain name <i>string</i>
Tree	keychain
Description	List of system keychains
Configurable	True
Max. Elements	1024

name *string*

Context	system authentication keychain name <i>string</i>
Description	The user configured name for the keychain
String Length	1 to 255
Configurable	True

admin-state *keyword*

Context	system authentication keychain name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Description	When set to disable, the keychain is inactive. When a protocol refers to a keychain that is inactive, no authentication data is added to the outbound messages and all inbound messages with authentication data are dropped. A key chain is also inactive if no key is configured.
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

description *string*

Context	system authentication keychain name <i>string</i> description <i>string</i>
Tree	description
Description	The user configured description for the keychain
String Length	1 to 255
Configurable	True

key index *number*

Context	system authentication keychain name <i>string</i> key index <i>number</i>
Tree	key
Description	List of keys in the keychain
Configurable	True
Max. Elements	1

index *number*

Context	system authentication keychain name <i>string</i> key index <i>number</i>
Description	Each key in a keychain requires a unique identifier. The index value specifies this identifier.
Configurable	True

algorithm *keyword*

Context	system authentication keychain name <i>string</i> key index <i>number</i> algorithm <i>keyword</i>
Tree	algorithm
Description	The cryptographic algorithm used with the keying material to secure the messages.
Options	<ul style="list-style-type: none">• cleartext The authentication-key is encoded in plaintext.• md5 The authentication-key is used to generate an MD5 digest (RFC 1321).• hmac-md5 The authentication-key is used to generate a 16-byte (128 bit) MD5 digest using the HMAC algorithm (RFC 2104).• hmac-sha-1 The authentication-key is used to generate a SHA1 digest using the HMAC algorithm (RFC 2104).• hmac-sha-256

The authentication-key is used to generate a SHA2 digest using the HMAC algorithm (RFC 2104). The SHA-256 variant of SHA2 produces an output of 32 bytes (256 bits).

- aes-128-cmac

The authentication-key is used with the AES-128 encryption algorithm to generate a cipher MAC (RFC 4493).

Configurable True

authentication-key *string*

Context **system authentication keychain name** *string* **key index** *number* **authentication-key** *string*

Tree **authentication-key**

Description The secret key.

The maximum string length is 25 characters, of which a maximum of 20 characters is the secret data and the remaining 5 characters, if provided, must be ' hash' (i.e. one whitespace plus the word hash). The trailing 'hash' keyword indicates that the secret data was already encrypted and this is the display version of that secret data, which is a hash of the original data. If the 'hash' keyword is omitted the string is assumed to be the actual secret data. Whenever the value of authentication-key is read by any management interface, from any datastore (candidate, running, state) the return value is always the encrypted value – i.e. with the trailing ' hash' characters included.

String Length 1 to 25

Configurable True

type *keyword*

Context **system authentication keychain name** *string* **type** *keyword*

Tree **type**

Description Specifies the intended use of the keychain. The type constrains the set of crypto algorithms that are available to use with each key in the keychain. It is also used ensure that this keychain is only used by protocols for which it is intended.

- Options
- tcp-md5
Keychain intended to be used for TCP-MD5 authentication.
 - isis
Keychain intended to be used for authentication of IS-IS PDUs.
 - ospf
Keychain intended to be used for authentication of OSPFv2 messages.
 - tcp-ao
Keychain intended to be used for TCP-AO authentication.

Configurable True

banner

Context	system banner
Tree	banner
Description	Contains configuration and state related to system banners
Configurable	True

login-banner *string*

Context	system banner login-banner <i>string</i>
Tree	login-banner
Description	Banner to display before a user has authenticated
Configurable	True

motd-banner *string*

Context	system banner motd-banner <i>string</i>
Tree	motd-banner
Description	Banner to display after a user has authenticated
Configurable	True

boot

Context	system boot
Tree	boot
Description	Top-level container for configuration and state data related to booting the system
Configurable	True

autoboot

Context	system boot autoboot
Tree	autoboot
Description	Top-level container for configuration and state data related to autobooting the system
Configurable	True

admin-state *keyword*

Context	system boot autoboot admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable autoboot functionality
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

attempts *number*

Context	system boot autoboot attempts <i>number</i>
Tree	attempts
Description	Sets the amount of executions to try autoboot, before rebooting the system
Range	1 to 10
Configurable	True

client-id *keyword*

Context	system boot autoboot client-id <i>keyword</i>
Tree	client-id
Description	The client ID to use on outgoing DHCP requests
Options	<ul style="list-style-type: none">• serial Use the chassis serial number as the client ID
Configurable	True

interface *reference*

Context	system boot autoboot interface <i>reference</i>
Tree	interface
Description	Sets the interface to use for autoboot functionality
Default	mgmt0
Reference	interface name <i>string</i>
Configurable	True

oper-state *string*

Context	system boot autoboot oper-state <i>string</i>
Tree	oper-state
Description	The current operational status of the autoboot process
Configurable	False

timeout *number*

Context	system boot autoboot timeout <i>number</i>
Tree	timeout
Description	Sets the timeout for each attempt to autoboot
Range	200 to 3600
Units	seconds
Configurable	True

image *string*

Context	system boot image <i>string</i>
Tree	image
Description	Ordered list of local images used to boot the system This directly translates into boot configuration in grub, where the images are tried in the order specified by the user. Images are sourced via the internal SD card, and the value passed is the folder that contains the initramfs, kernel, and squashfs image. The search path for these directories is /mnt/nokiaaos/<folder>
String Length	1 to 255
Configurable	True
Max. Elements	3

clock

Context	system clock
Tree	clock
Description	Top-level container for system clock configuration and state
Configurable	True

timezone *keyword*

Context	system clock timezone <i>keyword</i>
Tree	timezone
Description	The timezone to use for the system Based on IANAs Time Zone database
Options	<ul style="list-style-type: none">• Africa/Abidjan• Africa/Accra• Africa/Addis_Ababa• Africa/Algiers• Africa/Asmara• Africa/Bamako• Africa/Bangui• Africa/Banjul• Africa/Bissau• Africa/Blantyre• Africa/Brazzaville• Africa/Bujumbura• Africa/Cairo• Africa/Casablanca• Africa/Ceuta Ceuta, Melilla• Africa/Conakry• Africa/Dakar• Africa/Dar_es_Salaam• Africa/Djibouti• Africa/Douala• Africa/El_Aaiun• Africa/Freetown• Africa/Gaborone• Africa/Harare• Africa/Johannesburg• Africa/Juba• Africa/Kampala• Africa/Khartoum• Africa/Kigali• Africa/Kinshasa Dem. Rep. of Congo (west)• Africa/Lagos• Africa/Libreville• Africa/Lome

-
- Africa/Luanda
 - Africa/Lubumbashi
Dem. Rep. of Congo (east)
 - Africa/Lusaka
 - Africa/Malabo
 - Africa/Maputo
 - Africa/Maseru
 - Africa/Mbabane
 - Africa/Mogadishu
 - Africa/Monrovia
 - Africa/Nairobi
 - Africa/Ndjamena
 - Africa/Niamey
 - Africa/Nouakchott
 - Africa/Ouagadougou
 - Africa/Porto-Novo
 - Africa/Sao_Tome
 - Africa/Tripoli
 - Africa/Tunis
 - Africa/Windhoek
 - America/Adak
Aleutian Islands
 - America/Anchorage
Alaska (most areas)
 - America/Anguilla
 - America/Antigua
 - America/Araguaina
Tocantins
 - America/Argentina/Buenos_Aires
Buenos Aires (BA, CF)
 - America/Argentina/Catamarca
Catamarca (CT); Chubut (CH)
 - America/Argentina/Cordoba
Argentina (most areas: CB, CC, CN, ER, FM, MN, SE, SF)
 - America/Argentina/Jujuy
Jujuy (JY)
 - America/Argentina/La_Rioja
La Rioja (LR)
 - America/Argentina/Mendoza

-
- Mendoza (MZ)
 - America/Argentina/Rio_Gallegos
Santa Cruz (SC)
 - America/Argentina/Salta
Salta (SA, LP, NQ, RN)
 - America/Argentina/San_Juan
San Juan (SJ)
 - America/Argentina/San_Luis
San Luis (SL)
 - America/Argentina/Tucuman
Tucuman (TM)
 - America/Argentina/Ushuaia
Tierra del Fuego (TF)
 - America/Aruba
 - America/Asuncion
 - America/Atikokan
EST - ON (Atikokan); NU (Coral H)
 - America/Bahia
Bahia
 - America/Bahia_Banderas
Central Time - Bahia de Banderas
 - America/Barbados
 - America/Belem
Para (east); Amapa
 - America/Belize
 - America/Blanc-Sablon
AST - QC (Lower North Shore)
 - America/Boa_Vista
Roraima
 - America/Bogota
 - America/Boise
Mountain - ID (south); OR (east)
 - America/Cambridge_Bay
Mountain - NU (west)
 - America/Campo_Grande
Mato Grosso do Sul
 - America/Cancun
Eastern Standard Time - Quintana Roo
 - America/Caracas

-
- America/Cayenne
 - America/Cayman
 - America/Chicago
Central (most areas)
 - America/Chihuahua
Mountain Time - Chihuahua (most areas)
 - America/Costa_Rica
 - America/Creston
MST - BC (Creston)
 - America/Cuiaba
Mato Grosso
 - America/Curacao
 - America/Danmarkshavn
National Park (east coast)
 - America/Dawson
Pacific - Yukon (north)
 - America/Dawson_Creek
MST - BC (Dawson Cr, Ft St John)
 - America/Denver
Mountain (most areas)
 - America/Detroit
Eastern - MI (most areas)
 - America/Dominica
 - America/Edmonton
Mountain - AB; BC (E); SK (W)
 - America/Eirunepe
Amazonas (west)
 - America/El_Salvador
 - America/Fort_Nelson
MST - BC (Ft Nelson)
 - America/Fortaleza
Brazil (northeast: MA, PI, CE, RN, PB)
 - America/Glace_Bay
Atlantic - NS (Cape Breton)
 - America/Godthab
Greenland (most areas)
 - America/Goose_Bay
Atlantic - Labrador (most areas)
 - America/Grand_Turk

-
- America/Grenada
 - America/Guadeloupe
 - America/Guatemala
 - America/Guayaquil
Ecuador (mainland)
 - America/Guyana
 - America/Halifax
Atlantic - NS (most areas); PE
 - America/Havana
 - America/Hermosillo
Mountain Standard Time - Sonora
 - America/Indiana/Indianapolis
Eastern - IN (most areas)
 - America/Indiana/Knox
Central - IN (Starke)
 - America/Indiana/Marengo
Eastern - IN (Crawford)
 - America/Indiana/Petersburg
Eastern - IN (Pike)
 - America/Indiana/Tell_City
Central - IN (Perry)
 - America/Indiana/Vevay
Eastern - IN (Switzerland)
 - America/Indiana/Vincennes
Eastern - IN (Da, Du, K, Mn)
 - America/Indiana/Winamac
Eastern - IN (Pulaski)
 - America/Inuvik
Mountain - NT (west)
 - America/Iqaluit
Eastern - NU (most east areas)
 - America/Jamaica
 - America/Juneau
Alaska - Juneau area
 - America/Kentucky/Louisville
Eastern - KY (Louisville area)
 - America/Kentucky/Monticello
Eastern - KY (Wayne)
 - America/Kralendijk

-
- America/La_Paz
 - America/Lima
 - America/Los_Angeles
Pacific
 - America/Lower_Princes
 - America/Maceio
Alagoas, Sergipe
 - America/Managua
 - America/Manaus
Amazonas (east)
 - America/Marigot
 - America/Martinique
 - America/Matamoros
Central Time US - Coahuila, Nuevo Leon, Tamaulipas (US border)
 - America/Mazatlan
Mountain Time - Baja California Sur, Nayarit, Sinaloa
 - America/Menominee
Central - MI (Wisconsin border)
 - America/Merida
Central Time - Campeche, Yucatan
 - America/Metlakatla
Alaska - Annette Island
 - America/Mexico_City
Central Time
 - America/Miquelon
 - America/Moncton
Atlantic - New Brunswick
 - America/Monterrey
Central Time - Durango; Coahuila, Nuevo Leon, Tamaulipas (most areas)
 - America/Montevideo
 - America/Montserrat
 - America/Nassau
 - America/New_York
Eastern (most areas)
 - America/Nipigon
Eastern - ON, QC (no DST 1967-73)
 - America/Nome
Alaska (west)
 - America/Noronha

-
- Atlantic islands
 - America/North_Dakota/Beulah
Central - ND (Mercer)
 - America/North_Dakota/Center
Central - ND (Oliver)
 - America/North_Dakota/New_Salem
Central - ND (Morton rural)
 - America/Ojinaga
Mountain Time US - Chihuahua (US border)
 - America/Panama
 - America/Pangnirtung
Eastern - NU (Pangnirtung)
 - America/Paramaribo
 - America/Phoenix
MST - Arizona (except Navajo)
 - America/Port-au-Prince
 - America/Port_of_Spain
 - America/Porto_Velho
Rondonia
 - America/Puerto_Rico
 - America/Punta_Arenas
Region of Magallanes
 - America/Rainy_River
Central - ON (Rainy R, Ft Frances)
 - America/Rankin_Inlet
Central - NU (central)
 - America/Recife
Pernambuco
 - America/Regina
CST - SK (most areas)
 - America/Resolute
Central - NU (Resolute)
 - America/Rio_Branco
Acre
 - America/Santarem
Para (west)
 - America/Santiago
Chile (most areas)
 - America/Santo_Domingo

-
- America/Sao_Paulo
Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS)
 - America/Scoresbysund
Scoresbysund/Ittoqqortoormiit
 - America/Sitka
Alaska - Sitka area
 - America/St_Barthelemy
 - America/St_Johns
Newfoundland; Labrador (southeast)
 - America/St_Kitts
 - America/St_Lucia
 - America/St_Thomas
 - America/St_Vincent
 - America/Swift_Current
CST - SK (midwest)
 - America/Tegucigalpa
 - America/Thule
Thule/Pituffik
 - America/Thunder_Bay
Eastern - ON (Thunder Bay)
 - America/Tijuana
Pacific Time US - Baja California
 - America/Toronto
Eastern - ON, QC (most areas)
 - America/Tortola
 - America/Vancouver
Pacific - BC (most areas)
 - America/Whitehorse
Pacific - Yukon (south)
 - America/Winnipeg
Central - ON (west); Manitoba
 - America/Yakutat
Alaska - Yakutat
 - America/Yellowknife
Mountain - NT (central)
 - Antarctica/Casey
Casey
 - Antarctica/Davis
Davis

-
- Antarctica/DumontDURville
Dumont-d'Urville
 - Antarctica/Macquarie
Macquarie Island
 - Antarctica/Mawson
Mawson
 - Antarctica/McMurdo
New Zealand time - McMurdo, South Pole
 - Antarctica/Palmer
Palmer
 - Antarctica/Rothera
Rothera
 - Antarctica/Syowa
Syowa
 - Antarctica/Troll
Troll
 - Antarctica/Vostok
Vostok
 - Arctic/Longyearbyen
 - Asia/Aden
 - Asia/Almaty
Kazakhstan (most areas)
 - Asia/Amman
 - Asia/Anadyr
MSK+09 - Bering Sea
 - Asia/Aqtau
Mangghystau/Mankistau
 - Asia/Aqtobe
Aqtobe/Aktobe
 - Asia/Ashgabat
 - Asia/Atyrau
Atyrau/Atirau/Gur'yev
 - Asia/Baghdad
 - Asia/Bahrain
 - Asia/Baku
 - Asia/Bangkok
 - Asia/Barnaul
MSK+04 - Altai
 - Asia/Beirut

-
- Asia/Bishkek
 - Asia/Brunei
 - Asia/Chita
MSK+06 - Zabaykalsky
 - Asia/Choibalsan
Dornod, Sukhbaatar
 - Asia/Colombo
 - Asia/Damascus
 - Asia/Dhaka
 - Asia/Dili
 - Asia/Dubai
 - Asia/Dushanbe
 - Asia/Famagusta
Northern Cyprus
 - Asia/Gaza
Gaza Strip
 - Asia/Hebron
West Bank
 - Asia/Ho_Chi_Minh
 - Asia/Hong_Kong
 - Asia/Hovd
Bayan-Olgii, Govi-Altai, Hovd, Uvs, Zavkhan
 - Asia/Irkutsk
MSK+05 - Irkutsk, Buryatia
 - Asia/Jakarta
Java, Sumatra
 - Asia/Jayapura
New Guinea (West Papua / Irian Jaya); Maluku/Moluccas
 - Asia/Jerusalem
 - Asia/Kabul
 - Asia/Kamchatka
MSK+09 - Kamchatka
 - Asia/Karachi
 - Asia/Kathmandu
 - Asia/Khandyga
MSK+06 - Tomponsky, Ust-Maysky
 - Asia/Kolkata
 - Asia/Krasnoyarsk
MSK+04 - Krasnoyarsk area

-
- Asia/Kuala_Lumpur
Malaysia (peninsula)
 - Asia/Kuching
Sabah, Sarawak
 - Asia/Kuwait
 - Asia/Macau
 - Asia/Magadan
MSK+08 - Magadan
 - Asia/Makassar
Borneo (east, south); Sulawesi/Celebes, Bali, Nusa Tenggara; Timor (west)
 - Asia/Manila
 - Asia/Muscat
 - Asia/Nicosia
Cyprus (most areas)
 - Asia/Novokuznetsk
MSK+04 - Kemerovo
 - Asia/Novosibirsk
MSK+04 - Novosibirsk
 - Asia/Omsk
MSK+03 - Omsk
 - Asia/Oral
West Kazakhstan
 - Asia/Phnom_Penh
 - Asia/Pontianak
Borneo (west, central)
 - Asia/Pyongyang
 - Asia/Qatar
 - Asia/Qostanay
Qostanay/Kostanay/Kustanay
 - Asia/Qyzylorda
Qyzylorda/Kyzylorda/Kzyl-Orda
 - Asia/Riyadh
 - Asia/Sakhalin
MSK+08 - Sakhalin Island
 - Asia/Samarkand
Uzbekistan (west)
 - Asia/Seoul
 - Asia/Shanghai
Beijing Time

-
- Asia/Singapore
 - Asia/Srednekolymsk
MSK+08 - Sakha (E); North Kuril Is
 - Asia/Taipei
 - Asia/Tashkent
Uzbekistan (east)
 - Asia/Tbilisi
 - Asia/Tehran
 - Asia/Thimphu
 - Asia/Tokyo
 - Asia/Tomsk
MSK+04 - Tomsk
 - Asia/Ulaanbaatar
Mongolia (most areas)
 - Asia/Urumqi
Xinjiang Time
 - Asia/Ust-Nera
MSK+07 - Oymyakonsky
 - Asia/Vientiane
 - Asia/Vladivostok
MSK+07 - Amur River
 - Asia/Yakutsk
MSK+06 - Lena River
 - Asia/Yangon
 - Asia/Yekaterinburg
MSK+02 - Urals
 - Asia/Yerevan
 - Atlantic/Azores
Azores
 - Atlantic/Bermuda
 - Atlantic/Canary
Canary Islands
 - Atlantic/Cape_Verde
 - Atlantic/Faroe
 - Atlantic/Madeira
Madeira Islands
 - Atlantic/Reykjavik
 - Atlantic/South_Georgia
 - Atlantic/St_Helena

-
- Atlantic/Stanley
 - Australia/Adelaide
South Australia
 - Australia/Brisbane
Queensland (most areas)
 - Australia/Broken_Hill
New South Wales (Yancowinna)
 - Australia/Currie
Tasmania (King Island)
 - Australia/Darwin
Northern Territory
 - Australia/Eucla
Western Australia (Eucla)
 - Australia/Hobart
Tasmania (most areas)
 - Australia/Lindeman
Queensland (Whitsunday Islands)
 - Australia/Lord_Howe
Lord Howe Island
 - Australia/Melbourne
Victoria
 - Australia/Perth
Western Australia (most areas)
 - Australia/Sydney
New South Wales (most areas)
 - Europe/Amsterdam
 - Europe/Andorra
 - Europe/Astrakhan
MSK+01 - Astrakhan
 - Europe/Athens
 - Europe/Belgrade
 - Europe/Berlin
Germany (most areas)
 - Europe/Bratislava
 - Europe/Brussels
 - Europe/Bucharest
 - Europe/Budapest
 - Europe/Busingen
Busingen

-
- Europe/Chisinau
 - Europe/Copenhagen
 - Europe/Dublin
 - Europe/Gibraltar
 - Europe/Guernsey
 - Europe/Helsinki
 - Europe/Isle_of_Man
 - Europe/Istanbul
 - Europe/Jersey
 - Europe/Kaliningrad
MSK-01 - Kaliningrad
 - Europe/Kiev
Ukraine (most areas)
 - Europe/Kirov
MSK+00 - Kirov
 - Europe/Lisbon
Portugal (mainland)
 - Europe/Ljubljana
 - Europe/London
 - Europe/Luxembourg
 - Europe/Madrid
Spain (mainland)
 - Europe/Malta
 - Europe/Mariehamn
 - Europe/Minsk
 - Europe/Monaco
 - Europe/Moscow
MSK+00 - Moscow area
 - Europe/Oslo
 - Europe/Paris
 - Europe/Podgorica
 - Europe/Prague
 - Europe/Riga
 - Europe/Rome
 - Europe/Samara
MSK+01 - Samara, Udmurtia
 - Europe/San_Marino
 - Europe/Sarajevo
 - Europe/Saratov

-
- MSK+01 - Saratov
 - Europe/Simferopol
 - MSK+00 - Crimea
 - Europe/Skopje
 - Europe/Sofia
 - Europe/Stockholm
 - Europe/Tallinn
 - Europe/Tirane
 - Europe/Ulyanovsk
 - MSK+01 - Ulyanovsk
 - Europe/Uzhgorod
 - Ruthenia
 - Europe/Vaduz
 - Europe/Vatican
 - Europe/Vienna
 - Europe/Vilnius
 - Europe/Volgograd
 - MSK+01 - Volgograd
 - Europe/Warsaw
 - Europe/Zagreb
 - Europe/Zaporozhye
 - Zaporozh'ye/Zaporizhia; Lugansk/Luhansk (east)
 - Europe/Zurich
 - Indian/Antananarivo
 - Indian/Chagos
 - Indian/Christmas
 - Indian/Cocos
 - Indian/Comoro
 - Indian/Kerguelen
 - Indian/Mahe
 - Indian/Maldives
 - Indian/Mauritius
 - Indian/Mayotte
 - Indian/Reunion
 - Pacific/Apia
 - Pacific/Auckland
 - New Zealand (most areas)
 - Pacific/Bougainville
 - Bougainville

- Pacific/Chatham
Chatham Islands
- Pacific/Chuuk
Chuuk/Truk, Yap
- Pacific/Easter
Easter Island
- Pacific/Efate
- Pacific/Enderbury
Phoenix Islands
- Pacific/Fakaofu
- Pacific/Fiji
- Pacific/Funafuti
- Pacific/Galapagos
Galapagos Islands
- Pacific/Gambier
Gambier Islands
- Pacific/Guadalcanal
- Pacific/Guam
- Pacific/Honolulu
Hawaii
- Pacific/Kiritimati
Line Islands
- Pacific/Kosrae
Kosrae
- Pacific/Kwajalein
Kwajalein
- Pacific/Majuro
Marshall Islands (most areas)
- Pacific/Marquesas
Marquesas Islands
- Pacific/Midway
Midway Islands
- Pacific/Nauru
- Pacific/Niue
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pago_Pago
- Pacific/Palau
- Pacific/Pitcairn

- Pacific/Pohnpei
Pohnpei/Ponape
- Pacific/Port_Moresby
Papua New Guinea (most areas)
- Pacific/Rarotonga
- Pacific/Saipan
- Pacific/Tahiti
Society Islands
- Pacific/Tarawa
Gilbert Islands
- Pacific/Tongatapu
- Pacific/Wake
Wake Island
- Pacific/Wallis
- UTC

Configurable True

configuration

Context [system configuration](#)

Tree [configuration](#)

Description Top-level container for configuration and state data related to the system configuration

Configurable True

candidate name *string*

Context [system configuration candidate name *string*](#)

Tree [candidate](#)

Description List of configuration candidates currently active

Configurable False

name *string*

Context [system configuration candidate name *string*](#)

Description Name of the configuration candidate

String Length 1 to 255

Configurable False

started *string*

Context	system configuration candidate name <i>string</i> started <i>string</i>
Tree	started
Description	Start date and time of the configuration session
Configurable	False

type *keyword*

Context	system configuration candidate name <i>string</i> type <i>keyword</i>
Tree	type
Description	Type of configuration candidate
Options	<ul style="list-style-type: none">• shared• private
Configurable	False

username *string*

Context	system configuration candidate name <i>string</i> username <i>string</i>
Tree	username
Description	User that started the configuration session
String Length	1 to 255
Configurable	False

checkpoint id *number*

Context	system configuration checkpoint id <i>number</i>
Tree	checkpoint
Description	List of current checkpoints present in the system
Configurable	False

id *number*

Context	system configuration checkpoint id <i>number</i>
Description	System generated ID for the checkpoint
Configurable	False

comment *string*

Context	system configuration checkpoint id <i>number</i> comment <i>string</i>
Tree	comment
Description	User provided annotations associated with the checkpoint
Configurable	False

created *string*

Context	system configuration checkpoint id <i>number</i> created <i>string</i>
Tree	created
Description	Date and time this checkpoint was created
Configurable	False

name *string*

Context	system configuration checkpoint id <i>number</i> name <i>string</i>
Tree	name
Description	User provided name of the checkpoint
Configurable	False

size *number*

Context	system configuration checkpoint id <i>number</i> size <i>number</i>
Tree	size
Description	Size of the checkpoint configuration file
Units	bytes
Configurable	False

username *string*

Context	system configuration checkpoint id <i>number</i> username <i>string</i>
Tree	username
Description	Username that created this checkpoint
String Length	1 to 255
Configurable	False

version *string*

Context	system configuration checkpoint id <i>number</i> version <i>string</i>
Tree	version
Description	System version that the checkpoint was generated on
Configurable	False

commit id *number*

Context	system configuration commit id <i>number</i>
Tree	commit
Description	List of configuration transactions
Configurable	False

id *number*

Context	system configuration commit id <i>number</i>
Description	System identifier for the commit
Configurable	False

comment *string*

Context	system configuration commit id <i>number</i> comment <i>string</i>
Tree	comment
Description	Operator provided comment associated with this commit
Configurable	False

ended *string*

Context	system configuration commit id <i>number</i> ended <i>string</i>
Tree	ended
Description	End date and time of the commit This field is not populated if the commit is in progress
Configurable	False

name *string*

Context	system configuration commit id <i>number</i> name <i>string</i>
Tree	name
Description	Name of the configuration candidate the commit was triggered from
String Length	1 to 255
Configurable	False

started *string*

Context	system configuration commit id <i>number</i> started <i>string</i>
Tree	started
Description	Start date and time of the commit
Configurable	False

status *keyword*

Context	system configuration commit id <i>number</i> status <i>keyword</i>
Tree	status
Description	Current status of the commit
Options	<ul style="list-style-type: none">• validating• publishing• unconfirmed• checkpoint• save• complete• reverting• failed
Configurable	False

type *keyword*

Context	system configuration commit id <i>number</i> type <i>keyword</i>
Tree	type
Description	Type of configuration candidate the commit was triggered from
Options	<ul style="list-style-type: none">• shared• private
Configurable	False

username *string*

Context	system configuration commit id <i>number</i> username <i>string</i>
Tree	username
Description	User that started the commit
String Length	1 to 255
Configurable	False

idle-timeout *number*

Context	system configuration idle-timeout <i>number</i>
Tree	idle-timeout
Description	The idle timeout of configuration candidates After this period of no activity, the candidate is emptied and removed from the system.
Default	10080
Units	minutes
Configurable	True

last-change *string*

Context	system configuration last-change <i>string</i>
Tree	last-change
Description	Date and time of the last successful commit Set to the time the configuration was loaded by management server, so is refreshed at boot time.
Configurable	False

max-candidates *number*

Context	system configuration max-candidates <i>number</i>
Tree	max-candidates
Description	The maximum number of combined private and shared candidates
Range	1 to 255
Default	10
Configurable	True

max-checkpoints *number*

Context	system configuration max-checkpoints <i>number</i>
Tree	max-checkpoints
Description	The number of checkpoints kept by the system
Range	1 to 255
Default	10
Configurable	True

session id *number*

Context	system configuration session id <i>number</i>
Tree	session
Description	List of configuration sessions currently active
Configurable	False

id *number*

Context	system configuration session id <i>number</i>
Description	System generated ID for the configuration session
Configurable	False

exclusive *boolean*

Context	system configuration session id <i>number</i> exclusive <i>boolean</i>
Tree	exclusive
Description	Details if this session is running in exclusive mode
Configurable	False

name *string*

Context	system configuration session id <i>number</i> name <i>string</i>
Tree	name
Description	Name of the candidate the session is active on Set to 'default' if a non-named candidate is active
String Length	1 to 255
Configurable	False

started *string*

Context	system configuration session id <i>number</i> started <i>string</i>
Tree	started
Description	Start date and time of the configuration session
Configurable	False

type *keyword*

Context	system configuration session id <i>number</i> type <i>keyword</i>
Tree	type
Description	Type of configuration session
Options	<ul style="list-style-type: none">• shared• private
Configurable	False

username *string*

Context	system configuration session id <i>number</i> username <i>string</i>
Tree	username
Description	User that started the configuration session
Configurable	False

dns

Context	system dns
Tree	dns
Description	Top-level container for DNS configuration and state
Configurable	True

host-entry name *string*

Context	system dns host-entry name <i>string</i>
Tree	host-entry
Description	List of static host entries
Configurable	True

name *string*

Context	system dns host-entry name <i>string</i>
Description	Name of host entry
String Length	1 to 253
Configurable	True

ipv4-address *string*

Context	system dns host-entry name <i>string</i> ipv4-address <i>string</i>
Tree	ipv4-address
Description	IPv4 address for the host entry
Configurable	True

ipv6-address *string*

Context	system dns host-entry name <i>string</i> ipv6-address <i>string</i>
Tree	ipv6-address
Description	IPv6 address for the host entry
Configurable	True

network-instance *reference*

Context	system dns network-instance <i>reference</i>
Tree	network-instance
Description	Reference to a configured network-instance to source DNS requests from
Reference	network-instance name <i>string</i>
Configurable	True

oper-state *keyword*

Context	system dns oper-state <i>keyword</i>
Tree	oper-state
Description	Details the operational state of the DNS client
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational

- empty
Component slot is empty
- downloading
Component is downloading image into memory
- booting
Component is booting downloaded image
- starting
Component image operational, application processes starting
- failed
Component or process has failed
- synchronizing
Component is currently being synchronized
- upgrading
Component is currently being upgraded

Configurable False

search-list *string*

Context **system dns search-list** *string*

Tree **search-list**

Description An ordered list of domains to search when resolving a host name

String Length 1 to 253

Configurable True

server-list (*ipv4-address | ipv6-address*)

Context **system dns server-list** (*ipv4-address | ipv6-address*)

Tree **server-list**

Description List of the DNS servers that the resolver should query

Configurable True

Max. Elements 3

features *string*

Context	system features <i>string</i>
Tree	features
Description	Features enabled on this platform
String Length	1 to 255
Configurable	False
Introduced	20.6.1

ftp-server

Context	system ftp-server
Tree	ftp-server
Description	Top-level container for FTP server configuration and state
Configurable	True

network-instance [name](#) *reference*

Context	system ftp-server network-instance name <i>reference</i>
Tree	network-instance
Description	List of network-instances to run an FTP server in
Configurable	True

name *reference*

Context	system ftp-server network-instance name <i>reference</i>
Description	Reference to a configured network-instance
Reference	network-instance name <i>string</i>
Configurable	True

admin-state *keyword*

Context	system ftp-server network-instance name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Enables or disables the FTP server in this network-instance
Default	disable
Options	<ul style="list-style-type: none">enable

- disable
- Configurable True

oper-state *keyword*

- Context **system ftp-server network-instance name** *reference oper-state keyword*
- Tree **oper-state**
- Description Details the operational state of the FTP server
- Options
- up
Component or process is operational
 - down
Component or process is not operational
 - empty
Component slot is empty
 - downloading
Component is downloading image into memory
 - booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing
Component is currently being synchronized
 - upgrading
Component is currently being upgraded
- Configurable False

session-limit *number*

- Context **system ftp-server network-instance name** *reference session-limit number*
- Tree **session-limit**
- Description Set a limit on the number of simultaneous active FTP sessions
- Default 20
- Configurable True

source-address (*ipv4-address | ipv6-address*)

Context	system ftp-server network-instance name <i>reference</i> source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Description	IPv4 or IPv6 address for the FTP server to listen on within the network-instance Default behavior is to listen on '::', which will listen on all addresses for both IPv4 and IPv6. In order to listen on IPv4 only, this field should be set to '0.0.0.0'.
Default	::
Configurable	True

timeout *number*

Context	system ftp-server network-instance name <i>reference</i> timeout <i>number</i>
Tree	timeout
Description	Set the idle timeout in seconds on FTP connections
Default	300
Units	seconds
Configurable	True

gnmi-server

Context	system gnmi-server
Tree	gnmi-server
Description	Configures the gNMI server access API
Configurable	True

admin-state *keyword*

Context	system gnmi-server admin-state <i>keyword</i>
Tree	admin-state
Description	Globally enable or disable the gNMI server Disabling this will disable all gNMI servers.
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

commit-confirmed-timeout *number*

Context	system gnmi-server commit-confirmed-timeout <i>number</i>
Tree	commit-confirmed-timeout
Description	Number of seconds to wait for confirmation. A value of 0 means commit confirmed is not used
Range	0 to 86400
Default	0
Units	seconds
Configurable	True

network-instance [name](#) *reference*

Context	system gnmi-server network-instance name <i>reference</i>
Tree	network-instance
Description	List of network instances to run a gNMI server in
Configurable	True

name *reference*

Context	system gnmi-server network-instance name <i>reference</i>
Description	Reference to a configured network instance
Reference	network-instance name <i>string</i>
Configurable	True

admin-state *keyword*

Context	system gnmi-server network-instance name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the gNMI server
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system gnmi-server network-instance name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
Description	Details if the gNMI server is operationally available
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

port *number*

Context	system gnmi-server network-instance name <i>reference</i> port <i>number</i>
Tree	port
Description	Port the gNMI server will listen on for incoming connections
Range	0 to 65535
Default	57400
Configurable	True

source-address (*ipv4-address | ipv6-address*)

Context	system gnmi-server network-instance name <i>reference</i> source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Description	List of IP addresses the gNMI server will listen on within the network instance
Default	::
Configurable	True

tls-profile *reference*

Context	system gnmi-server network-instance name <i>reference</i> tls-profile <i>reference</i>
Tree	tls-profile
Description	Reference to the TLS profile to use on the gNMI server
Reference	system tls server-profile name <i>string</i>
Configurable	True

use-authentication *boolean*

Context	system gnmi-server network-instance name <i>reference</i> use-authentication <i>boolean</i>
Tree	use-authentication
Description	Enable or disable the use of username/password authentication for every gNMI request
Default	true
Configurable	True

rate-limit *number*

Context	system gnmi-server rate-limit <i>number</i>
Tree	rate-limit
Description	Set a limit on the number of connection attempts per minute
Range	0 to 65535
Default	60
Configurable	True

session-limit *number*

Context	system gnmi-server session-limit <i>number</i>
Tree	session-limit
Description	Set a limit on the number of simultaneous active gNMI sessions
Range	0 to 65535
Default	20
Configurable	True

subscription id *number*

Context	system gnmi-server subscription id <i>number</i>
Tree	subscription
Description	List of subscriptions
Configurable	False

id *number*

Context	system gnmi-server subscription id <i>number</i>
Description	System generated ID for for the subscription
Range	0 to 4294967295
Configurable	False

mode *keyword*

Context	system gnmi-server subscription id <i>number</i> mode <i>keyword</i>
Tree	mode
Description	Subscription mode (ON_CHANGE, SAMPLE, TARGET_DEFINED, POLL, ONCE)
Options	<ul style="list-style-type: none">• ON_CHANGE• SAMPLE• TARGET_DEFINED• POLL• ONCE
Configurable	False

paths *string*

Context	system gnmi-server subscription id <i>number</i> paths <i>string</i>
Tree	paths
Description	List of paths being subscribed to
Configurable	False

remote-host (*ipv4-address | ipv6-address*)

Context	system gnmi-server subscription id <i>number</i> remote-host (<i>ipv4-address ipv6-address</i>)
Tree	remote-host
Description	Remote host of the subscription
Configurable	False

remote-port *number*

Context	system gnmi-server subscription id <i>number</i> remote-port <i>number</i>
Tree	remote-port
Description	Remote port of the subscription
Range	0 to 65535
Configurable	False

sample-interval *number*

Context	system gnmi-server subscription id <i>number</i> sample-interval <i>number</i>
Tree	sample-interval
Description	Time in seconds to provide updates to the remote host, set to 0 for all subscription modes except SAMPLE
Units	seconds
Configurable	False

start-time *string*

Context	system gnmi-server subscription id <i>number</i> start-time <i>string</i>
Tree	start-time
Description	Time of the subscription creation
Configurable	False

user *string*

Context	system gnmi-server subscription id <i>number</i> user <i>string</i>
Tree	user
Description	Authenticated username for the subscription
Configurable	False

user-agent *string*

Context	system gnmi-server subscription id <i>number</i> user-agent <i>string</i>
Tree	user-agent
Description	User agent used for the subscription
Configurable	False

timeout *number*

Context	system gnmi-server timeout <i>number</i>
Tree	timeout
Description	Set the idle timeout in seconds on gNMI connections
Range	0 to 65535
Default	7200
Units	seconds
Configurable	True

trace-options *keyword*

Context	system gnmi-server trace-options <i>keyword</i>
Tree	trace-options
Description	gNMI trace options
Options	<ul style="list-style-type: none">• request• response• common
Configurable	True

unix-socket

Context	system gnmi-server unix-socket
Tree	unix-socket
Description	Top-level container for configuration and state related to unix sockets
Configurable	True

admin-state *keyword*

Context	system gnmi-server unix-socket admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the gNMI server
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system gnmi-server unix-socket oper-state <i>keyword</i>
Tree	oper-state
Description	Details if the gNMI server is operationally available
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading

Component is currently being upgraded

Configurable False

socket-path *string*

Context [system gnmi-server unix-socket socket-path](#) *string*

Tree [socket-path](#)

Description Path to the unix socket used by gNMI

Configurable False

tls-profile *reference*

Context [system gnmi-server unix-socket tls-profile](#) *reference*

Tree [tls-profile](#)

Description Reference to the TLS profile to use on the gNMI unix socket server
If none is specified, then TLS is not used.

Reference [system tls server-profile name](#) *string*

Configurable True

use-authentication *boolean*

Context [system gnmi-server unix-socket use-authentication](#) *boolean*

Tree [use-authentication](#)

Description Enable or disable the use of username/password authentication for every gNMI request

Default true

Configurable True

information

Context [system information](#)

Tree [information](#)

Description Top-level container for system information configuration and state

Configurable True

contact *string*

Context	system information contact <i>string</i>
Tree	contact
Description	The system contact This field represents contact information for the person or group that maintains the system. This field is exposed via SNMP at the sysContact OID.
Configurable	True

current-datetime *string*

Context	system information current-datetime <i>string</i>
Tree	current-datetime
Description	The current system date and time
Configurable	False

description *string*

Context	system information description <i>string</i>
Tree	description
Description	The system description This field is system generated, and is a combination of the system host name, software version, kernel version, and build date. The template for this field is: SRLinux-<version> <hostname> <kernel> <build date>. This field is exposed via SNMP at the sysDescr OID.
Configurable	False

location *string*

Context	system information location <i>string</i>
Tree	location
Description	The system location This field represents the location of the system, and is commonly used by inventory management systems to group elements together. This field is exposed via SNMP at the sysLocation OID.
Configurable	True

uptime *string*

Context	system information uptime <i>string</i>
Tree	uptime
Description	The time the system has been operational The system is considered operational when the active control card has become operational
Configurable	False

version *string*

Context	system information version <i>string</i>
Tree	version
Description	The system version This field represents the version of the management server
Configurable	False

ip-load-balancing

Context	system ip-load-balancing
Tree	ip-load-balancing
Description	
Configurable	True

hash-keys

Context	system ip-load-balancing hash-keys
Tree	hash-keys
Description	Container for hash-keys that will be used to load-balance IP traffic across IP next-hops that form an ECMP set
Configurable	True

hash-seed *number*

Context	system ip-load-balancing hash-keys hash-seed <i>number</i>
Tree	hash-seed
Description	A configured hash seed to override the default value of 0

When different routers have a different hash-seed traffic polarization effects can be minimized.

Default 0
Configurable True

json-rpc-server

Context [system json-rpc-server](#)
Tree [json-rpc-server](#)
Description Configures the JSON RPC access API
Configurable True

admin-state *keyword*

Context [system json-rpc-server admin-state](#) *keyword*
Tree [admin-state](#)
Description Globally enable or disable the JSON RPC server Disabling this will disable all JSON RPC servers.
Default disable
Options

- enable
- disable

Configurable True

commit-confirmed-timeout *number*

Context [system json-rpc-server commit-confirmed-timeout](#) *number*
Tree [commit-confirmed-timeout](#)
Description Number of seconds to wait for confirmation. A value of 0 means commit confirmed is not used
Range 0 to 86400
Default 0
Units seconds
Configurable True

network-instance *name reference*

Context	system json-rpc-server network-instance name reference
Tree	network-instance
Description	List of network instances to run the JSON RPC server in
Configurable	True

name *reference*

Context	system json-rpc-server network-instance name reference
Description	Reference to a configured network-instance
Reference	network-instance name string
Configurable	True

http

Context	system json-rpc-server network-instance name reference http
Tree	http
Description	Top-level container for the JSON-RPC HTTP server
Configurable	True

admin-state *keyword*

Context	system json-rpc-server network-instance name reference http admin-state keyword
Tree	admin-state
Description	Administratively enable or disable the HTTP JSON RPC server This requires the JSON RPC server to be globally enabled
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system json-rpc-server network-instance name reference http oper-state keyword
Tree	oper-state
Description	Details if the JSON RPC server is operationally available
Options	<ul style="list-style-type: none">• up

	Component or process is operational
•	down
	Component or process is not operational
•	empty
	Component slot is empty
•	downloading
	Component is downloading image into memory
•	booting
	Component is booting downloaded image
•	starting
	Component image operational, application processes starting
•	failed
	Component or process has failed
•	synchronizing
	Component is currently being synchronized
•	upgrading
	Component is currently being upgraded
Configurable	False

port number

Context	system json-rpc-server network-instance name <i>reference</i> http port number
Tree	port
Description	The port the HTTP JSON RPC server will listen on for incoming connections
Range	0 to 65535
Default	80
Configurable	True

session-limit number

Context	system json-rpc-server network-instance name <i>reference</i> http session-limit number
Tree	session-limit
Description	The number of concurrent requests the server will allow. If a request comes in while this limit is reached, the request will block until another request is finished.
Range	1 to 100
Default	10
Configurable	True

source-address (*ipv4-address | ipv6-address*)

Context	system json-rpc-server network-instance name <i>reference</i> http source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Description	List of IP addresses the JSON RPC server will listen on within the network instance
Default	::
Configurable	True

use-authentication *boolean*

Context	system json-rpc-server network-instance name <i>reference</i> http use-authentication <i>boolean</i>
Tree	use-authentication
Description	Enable or disable the use of username/password authentication for every JSON RPC request
Default	true
Configurable	True

https

Context	system json-rpc-server network-instance name <i>reference</i> https
Tree	https
Description	Top-level container for the JSON-RPC HTTPS server
Configurable	True

admin-state *keyword*

Context	system json-rpc-server network-instance name <i>reference</i> https admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the HTTPS JSON RPC server This requires the JSON RPC server to be globally enabled
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system json-rpc-server network-instance name <i>reference</i> https oper-state <i>keyword</i>
Tree	oper-state
Description	Details if the JSON RPC server is operationally available
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

port *number*

Context	system json-rpc-server network-instance name <i>reference</i> https port <i>number</i>
Tree	port
Description	Port the HTTPS JSON RPC server will listen on for incoming connections
Range	0 to 65535
Default	443
Configurable	True

session-limit *number*

Context	system json-rpc-server network-instance name <i>reference</i> https session-limit <i>number</i>
Tree	session-limit
Description	The number of concurrent requests the server will allow. If a request comes in while this limit is reached, the request will block until another request is finished.
Range	1 to 100
Default	10
Configurable	True

source-address (*ipv4-address | ipv6-address*)

Context	system json-rpc-server network-instance name <i>reference</i> https source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Description	List of IP addresses the JSON RPC server will listen on within the network instance
Default	::
Configurable	True

tls-profile *reference*

Context	system json-rpc-server network-instance name <i>reference</i> https tls-profile <i>reference</i>
Tree	tls-profile
Description	Reference to the TLS profile to use on the HTTP JSON RPC server
Reference	system tls server-profile name <i>string</i>
Configurable	True

use-authentication *boolean*

Context	system json-rpc-server network-instance name <i>reference</i> https use-authentication <i>boolean</i>
Tree	use-authentication
Description	Enable or disable the use of username/password authentication for every JSON RPC request
Default	true
Configurable	True

trace-options *keyword*

Context	system json-rpc-server trace-options <i>keyword</i>
Tree	trace-options
Description	JSON RPC trace options
Options	<ul style="list-style-type: none">• request• response• common
Configurable	True

unix-socket

Context	system json-rpc-server unix-socket
Tree	unix-socket
Description	Top-level container for configuration and state related to unix sockets
Configurable	True

admin-state *keyword*

Context	system json-rpc-server unix-socket admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable the JSON RPC server via unix socket This requires the JSON RPC server to be globally enabled
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system json-rpc-server unix-socket oper-state <i>keyword</i>
Tree	oper-state
Description	Details if the JSON RPC server is operationally available
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty

	Component slot is empty
• downloading	Component is downloading image into memory
• booting	Component is booting downloaded image
• starting	Component image operational, application processes starting
• failed	Component or process has failed
• synchronizing	Component is currently being synchronized
• upgrading	Component is currently being upgraded
Configurable	False

socket-path *string*

Context	system json-rpc-server unix-socket socket-path <i>string</i>
Tree	socket-path
Description	Path to the unix socket used by JSON RPC
Configurable	False

tls-profile *reference*

Context	system json-rpc-server unix-socket tls-profile <i>reference</i>
Tree	tls-profile
Description	Reference to the TLS profile to use on the JSON RPC unix socket server If none is specified, then TLS is not used.
Reference	system tls server-profile name <i>string</i>
Configurable	True

use-authentication *boolean*

Context	system json-rpc-server unix-socket use-authentication <i>boolean</i>
Tree	use-authentication
Description	Enable or disable the use of username/password authentication for every JSON RPC request
Default	true
Configurable	True

lACP

Context	system lACP
Tree	lACP
Description	
Configurable	True

system-id *string*

Context	system lACP system-id <i>string</i>
Tree	system-id
Description	The MAC address portion of the node's System ID. This is combined with the system priority to construct the 8-octet system-id
Configurable	True

system-priority *number*

Context	system lACP system-priority <i>number</i>
Tree	system-priority
Description	System priority used by the node on this LAG interface. Lower value is higher priority for determining which node is the controlling system.
Configurable	True

lldp

Context	system lldp
Tree	lldp
Description	Top-level container for LLDP configuration and state data
Configurable	True

admin-state *keyword*

Context	system lldp admin-state <i>keyword</i>
Tree	admin-state
Description	Enable or disable LLDP at the system level
Default	enable
Options	<ul style="list-style-type: none">enable

- disable
- Configurable True

bgp-auto-discovery

- Context [system lldp bgp-auto-discovery](#)
- Tree [bgp-auto-discovery](#)
- Description Top-level container for global LLDP BGP auto discovery
- Configurable True

admin-state *keyword*

- Context [system lldp bgp-auto-discovery admin-state](#) *keyword*
- Tree [admin-state](#)
- Description Enable or disable LLDP BGP auto discovery at the system level
Setting this to disable will override any per-interface LLDP BGP autodiscovery configuration
- Default disable
- Options
 - enable
 - disable
- Configurable True

group-id *number*

- Context [system lldp bgp-auto-discovery group-id](#) *number*
- Tree [group-id](#)
- Description A four byte integer to send on outgoing LLDPDUs
This value can be used on the remote end to do peer group association. This sub-TLV is not sent by default
- Configurable True

network-instance *reference*

- Context [system lldp bgp-auto-discovery network-instance](#) *reference*
- Tree [network-instance](#)
- Description List of network instances to enable LLDP BGP auto discovery in

Default is to run LLDP BGP auto discovery in all network instances

Reference **network-instance name** *string*

Configurable True

chassis-id *string*

Context **system lldp chassis-id** *string*

Tree **chassis-id**

Description The Chassis ID is a mandatory TLV which identifies the chassis component of the endpoint identifier associated with the transmitting LLDP agent

Configurable False

chassis-id-type *keyword*

Context **system lldp chassis-id-type** *keyword*

Tree **chassis-id-type**

Description The source for the chassis identifier string
It is an enumerator defined by the LldpChassisIdSubtype object from IEEE 802.1AB MIB.

Default MAC_ADDRESS

- Options
- CHASSIS_COMPONENT
Chassis identifier based on the value of entPhysicalAlias object defined in IETF RFC 2737
 - INTERFACE_ALIAS
Chassis identifier based on the value of ifAlias object defined in IETF RFC 2863
 - PORT_COMPONENT
Chassis identifier based on the value of entPhysicalAlias object defined in IETF RFC 2737 for a port or backplane component
 - MAC_ADDRESS
Chassis identifier based on the value of a unicast source address (encoded in network byte order and IEEE 802.3 canonical bit order), of a port on the containing chassis as defined in IEEE Std 802-2001
 - NETWORK_ADDRESS
Chassis identifier based on a network address, associated with a particular chassis. The encoded address is composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value
 - INTERFACE_NAME
Chassis identifier based on the name of the interface, e.g., the value of ifName object defined in IETF RFC 2863
 - LOCAL

Chassis identifier based on a locally defined value

Configurable False

hello-timer *number*

Context [system lldp hello-timer](#) *number*
Tree [hello-timer](#)
Description System level hello timer for the LLDP protocol
Default 30
Units seconds
Configurable True

hold-multiplier *number*

Context [system lldp hold-multiplier](#) *number*
Tree [hold-multiplier](#)
Description System level hold multiplier, used to define neighbor aging
This field defines how many hellos need to be missed before a neighbor is aged out.
This field also is used along with the 'hello-timer' field to define the TTL TLV in outgoing LLDPDUs.
Default 4
Configurable True

interface name *reference*

Context [system lldp interface name](#) *reference*
Tree [interface](#)
Description List of interfaces on which LLDP can be enabled
Configurable True

name *reference*

Context [system lldp interface name](#) *reference*
Description Reference to the LLDP Ethernet interface
Reference [interface name](#) *string*
Configurable True

admin-state *keyword*

Context	system lldp interface name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Enable or disable LLDP on the interface
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

bgp-auto-discovery

Context	system lldp interface name <i>reference</i> bgp-auto-discovery
Tree	bgp-auto-discovery
Description	Configuration and state related to LLDP BGP auto discovery on the interface
Configurable	True

admin-state *keyword*

Context	system lldp interface name <i>reference</i> bgp-auto-discovery admin-state <i>keyword</i>
Tree	admin-state
Description	Enable or disable LLDP BGP auto discovery on this interface
Default	enable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

group-id *number*

Context	system lldp interface name <i>reference</i> bgp-auto-discovery group-id <i>number</i>
Tree	group-id
Description	A four byte integer to send on outgoing LLDPDU This value can be used on the remote end to do peer group association. This sub-TLV is not sent by default.
Configurable	True

peering-address (*ipv4-address | ipv6-address*)

Context	system lldp interface name <i>reference</i> bgp-auto-discovery peering-address (<i>ipv4-address ipv6-address</i>)
Tree	peering-address
Description	List of IP addresses to be sent for BGP auto discovery Default values for this sub-TLV is to populate the addresses of the first subinterface of the interface the LLDPDU is being generated from, along with a unicast AFI/SAFI for IPv4 if an IPv4 address exists, and/or IPv6 if an IPv6 address exists. If neither of these exist in the system, LLDP will not add the TLV to outgoing LLDPDUs, unless the peering-address is manually configured on a per-LLDP-port basis.
Configurable	True

neighbor id *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i>
Tree	neighbor
Description	List of LLDP neighbors on this interface
Configurable	False

id *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i>
Description	System generated identifier for the remote neighbor
Configurable	False

bgp-auto-discovery

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> bgp-auto-discovery
Tree	bgp-auto-discovery
Description	Enclosing container for BGP auto discovery
Configurable	False

bgp-peer-addresses *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> bgp-auto-discovery bgp-peer-addresses <i>string</i>
Tree	bgp-peer-addresses
Description	List of IP address learned from neighbor for BGP auto discovery
Configurable	False

group-id *number*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> bgp-auto-discovery group-id <i>number</i>
Tree	group-id
Description	A four byte integer to send on outgoing LLDPDUs, this value can be used on the remote end to do peer group association. This sub-TLV is not sent by default
Configurable	False

capability name *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> capability name <i>string</i>
Tree	capability
Description	List of LLDP system capabilities advertised by the neighbor
Configurable	False

name *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> capability name <i>string</i>
Description	Name of the system capability advertised by the neighbor Capabilities are represented in a bitmap that defines the primary functions of the system. The capabilities are defined in IEEE 802.1AB.
Configurable	False

enabled *boolean*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> capability name <i>string</i> enabled <i>boolean</i>
Tree	enabled
Description	Indicates whether the corresponding system capability is enabled on the neighbor
Configurable	False

chassis-id *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> chassis-id <i>string</i>
Tree	chassis-id
Description	The chassis ID of the remote neighbor The Chassis ID is a mandatory TLV which identifies the chassis component of the endpoint identifier associated with the transmitting LLDP agent
Configurable	False

chassis-id-type *keyword*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> chassis-id-type <i>keyword</i>
Tree	chassis-id-type
Description	The type of identifier used in the chassis-id field This field identifies the format and source of the chassis identifier string. It is an enumerator defined by the LldpChassisIdSubtype object from IEEE 802.1AB MIB.
Default	MAC_ADDRESS
Options	<ul style="list-style-type: none">• CHASSIS_COMPONENT Chassis identifier based on the value of entPhysicalAlias object defined in IETF RFC 2737• INTERFACE_ALIAS Chassis identifier based on the value of ifAlias object defined in IETF RFC 2863• PORT_COMPONENT Chassis identifier based on the value of entPhysicalAlias object defined in IETF RFC 2737 for a port or backplane component• MAC_ADDRESS Chassis identifier based on the value of a unicast source address (encoded in network byte order and IEEE 802.3 canonical bit order), of a port on the containing chassis as defined in IEEE Std 802-2001• NETWORK_ADDRESS Chassis identifier based on a network address, associated with a particular chassis. The encoded address is composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value• INTERFACE_NAME Chassis identifier based on the name of the interface, e.g., the value of ifName object defined in IETF RFC 2863• LOCAL Chassis identifier based on a locally defined value
Configurable	False

custom-tlv *type number oui string oui-subtype string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type <i>number</i> oui <i>string</i> oui-subtype <i>string</i>
Tree	custom-tlv
Description	List of custom LLDP TLVs from a neighbor
Configurable	False

type *number*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type <i>number</i> oui <i>string</i> oui-subtype <i>string</i>
Description	The integer value identifying the type of information contained in the value field.
Configurable	False

oui *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type <i>number</i> oui <i>string</i> oui-subtype <i>string</i>
Description	The organizationally unique identifier field from the custom TLV This field shall contain the organization's OUI as defined in Clause 9 of IEEE Std 802. The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the 'Assigned Numbers' RFC [RFC3232].
Configurable	False

oui-subtype *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type <i>number</i> oui <i>string</i> oui-subtype <i>string</i>
Description	The subtype value defined by the OUI for this custom TLV The organizationally defined subtype field shall contain a unique subtype value assigned by the defining organization.
Configurable	False

value *binary*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type <i>number</i> oui <i>string</i> oui-subtype <i>string</i> value <i>binary</i>
Tree	value
Description	A variable-length octet-string containing the value for this TLV
Configurable	False

first-message *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> first-message <i>string</i>
Tree	first-message
Description	Date and time of the first message from neighbor
Configurable	False

last-update *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> last-update <i>string</i>
Tree	last-update
Description	Date and time of the last update from neighbor
Configurable	False

management-address [address](#) *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> management-address address <i>string</i>
Tree	management-address
Description	List of management addresses received from the remote LLDP neighbor
Configurable	False

address *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> management-address address <i>string</i>
Description	The management address received from the remote LLDP neighbor The Management Address is a mandatory TLV which identifies a network address associated with the LLDP agent, which can be used to reach the agent on the port identified in the Port ID TLV.
Configurable	False

type *keyword*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> management-address address <i>string</i> type <i>keyword</i>
Tree	type
Description	The type of management address referenced in the address field The enumerated value for the network address type identified in this TLV. This enumeration is defined in the 'Assigned Numbers' RFC [RFC3232] and the ianaAddressFamilyNumbers object.
Options	<ul style="list-style-type: none">• IPv4 Use IPv4 address for management address type• IPv6 Use IPv6 address for management address type
Configurable	False

port-description *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> port-description <i>string</i>
Tree	port-description
Description	The description of the port referenced in the port-id field The binary string containing the actual port identifier for the port which this LLDP PDU was transmitted. The source and format of this field is defined by PtopoPortId from RFC2922.
Configurable	False

port-id (*string | binary*)

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> port-id (<i>string binary</i>)
Tree	port-id
Description	The Port ID of the remote neighbor The Port ID is a mandatory TLV which identifies the port component of the endpoint identifier associated with the transmitting LLDP agent. If the specified port is an IEEE 802.3 Repeater port, then this TLV is optional.
Configurable	False

port-id-type *keyword*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> port-id-type <i>keyword</i>
Tree	port-id-type
Description	The type of identifier used in the port-id field

This field identifies the format and source of the port identifier string. It is an enumerator defined by the PtopoPortIdType object from RFC2922.

Options	<ul style="list-style-type: none"> • INTERFACE_ALIAS Chassis identifier based on the value of ifAlias object defined in IETF RFC 2863 • PORT_COMPONENT Port identifier based on the value of entPhysicalAlias object defined in IETF RFC 2737 for a port component • MAC_ADDRESS Port identifier based on the value of a unicast source address (encoded in network byte order and IEEE 802.3 canonical bit order) associated with a port • NETWORK_ADDRESS Port identifier based on a network address, associated with a particular port • INTERFACE_NAME Port identifier based on the name of the interface, e.g., the value of ifName object defined in IETF RFC 2863 • AGENT_CIRCUIT_ID Port identifier based on the circuit id in the DHCP relay agent information option as defined in IETF RFC 3046 • LOCAL Port identifier based on a locally defined alphanumeric string
Configurable	False

system-description *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> system-description <i>string</i>
Tree	system-description
Description	<p>The system description of the remote neighbor</p> <p>The system description field shall contain an alpha-numeric string that is the textual description of the network entity. The system description should include the full name and version identification of the system's hardware type, software operating system, and networking software. If implementations support IETF RFC 3418, the sysDescr object should be used for this field.</p>
String Length	0 to 255
Configurable	False

system-name *string*

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> system-name <i>string</i>
Tree	system-name
Description	The administratively assigned name of the remote neighbor

The system name field shall contain an alpha-numeric string that indicates the system's administratively assigned name. The system name should be the system's fully qualified domain name. If implementations support IETF RFC 3418, the sysName object should be used for this field.

String Length 0 to 255

Configurable False

oper-state *keyword*

Context [system lldp interface name](#) *reference* [oper-state](#) *keyword*

Tree [oper-state](#)

Description Details the operational state of LLDP on the interface

- Options
- up
Component or process is operational
 - down
Component or process is not operational
 - empty
Component slot is empty
 - downloading
Component is downloading image into memory
 - booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing
Component is currently being synchronized
 - upgrading
Component is currently being upgraded

Configurable False

statistics

Context [system lldp interface name](#) *reference* [statistics](#)

Tree [statistics](#)

Description LLDP counters on each interface

Configurable False

frame-discard *number*

Context	system lldp interface name <i>reference</i> statistics frame-discard <i>number</i>
Tree	frame-discard
Description	The number of LLDP frames received and discarded
Default	0
Configurable	False

frame-error-in *number*

Context	system lldp interface name <i>reference</i> statistics frame-error-in <i>number</i>
Tree	frame-error-in
Description	The number of LLDP frames received with errors
Default	0
Configurable	False

frame-error-out *number*

Context	system lldp interface name <i>reference</i> statistics frame-error-out <i>number</i>
Tree	frame-error-out
Description	The number of frame transmit errors on the interface
Default	0
Configurable	False

frame-in *number*

Context	system lldp interface name <i>reference</i> statistics frame-in <i>number</i>
Tree	frame-in
Description	The number of LLDP frames received
Default	0
Configurable	False

frame-out *number*

Context	system lldp interface name <i>reference</i> statistics frame-out <i>number</i>
Tree	frame-out
Description	The number of LLDP frames transmitted
Default	0
Configurable	False

last-clear *string*

Context	system lldp interface name <i>reference</i> statistics last-clear <i>string</i>
Tree	last-clear
Description	Indicates the last time the counters were cleared
Configurable	False

tlv-discard *number*

Context	system lldp interface name <i>reference</i> statistics tlv-discard <i>number</i>
Tree	tlv-discard
Description	The number of TLV frames received and discarded
Default	0
Configurable	False

tlv-unknown *number*

Context	system lldp interface name <i>reference</i> statistics tlv-unknown <i>number</i>
Tree	tlv-unknown
Description	The number of frames received with unknown TLV
Default	0
Configurable	False

management-address [subinterface](#) *string*

Context	system lldp management-address subinterface <i>string</i>
Tree	management-address
Description	List of subinterfaces to source management addresses from This list is sent in the management address TLV by LLDP.
Configurable	True

subinterface *string*

Context	system lldp management-address subinterface <i>string</i>
Description	Reference to the subinterface to source management addresses
String Length	3 to 24
Configurable	True

type *keyword*

Context	system lldp management-address subinterface <i>string</i> type <i>keyword</i>
Tree	type
Description	Types of addresses sent in the management address TLV The enumerated value for the network address type identified in this TLV. This enumeration is defined in the 'Assigned Numbers' RFC [RFC3232] and the ianaAddressFamilyNumbers object.
Options	<ul style="list-style-type: none">• IPv4 Use IPv4 address for management address type• IPv6 Use IPv6 address for management address type
Configurable	True

statistics

Context	system lldp statistics
Tree	statistics
Description	Global LLDP counters
Configurable	False

entries-aged-out *number*

Context	system lldp statistics entries-aged-out <i>number</i>
Tree	entries-aged-out
Description	The number of entries aged out due to timeout.
Default	0
Configurable	False

frame-discard *number*

Context	system lldp statistics frame-discard <i>number</i>
Tree	frame-discard
Description	The number of LLDP frames received and discarded
Default	0
Configurable	False

frame-error-in *number*

Context	system lldp statistics frame-error-in <i>number</i>
Tree	frame-error-in
Description	The number of LLDP frames received with errors
Default	0
Configurable	False

frame-in *number*

Context	system lldp statistics frame-in <i>number</i>
Tree	frame-in
Description	The number of LLDP frames received
Default	0
Configurable	False

frame-out *number*

Context	system lldp statistics frame-out <i>number</i>
Tree	frame-out
Description	The number of LLDP frames transmitted
Default	0
Configurable	False

last-clear *string*

Context	system lldp statistics last-clear <i>string</i>
Tree	last-clear
Description	Indicates the last time the counters were cleared
Configurable	False

tlv-accepted *number*

Context	system lldp statistics tlv-accepted <i>number</i>
Tree	tlv-accepted
Description	The number of valid TLVs received.
Default	0
Configurable	False

tlv-discard *number*

Context	system lldp statistics tlv-discard <i>number</i>
Tree	tlv-discard
Description	The number of TLV frames received and discarded
Default	0
Configurable	False

tlv-unknown *number*

Context	system lldp statistics tlv-unknown <i>number</i>
Tree	tlv-unknown
Description	The number of frames received with unknown TLV
Default	0
Configurable	False

system-description *string*

Context	system lldp system-description <i>string</i>
Tree	system-description
Description	Field detailing system description, including name and versions The system description field shall contain an alpha-numeric string that is the textual description of the network entity. The system description should include the full name and version identification of the system's hardware type, software operating system, and networking software.
String Length	0 to 255
Configurable	False

system-name *string*

Context	system lldp system-name <i>string</i>
Tree	system-name
Description	The systems administratively assigned name The system name field shall contain an alpha-numeric string that indicates the system's administratively assigned name. The system name should be the system's fully qualified domain name.
String Length	0 to 255
Configurable	False

trace-options *keyword*

Context	system lldp trace-options <i>keyword</i>
Tree	trace-options
Description	LLDP trace options
Options	<ul style="list-style-type: none">• received• transmitted• common
Configurable	True

logging

Context	system logging
Tree	logging
Description	System logging provides the interface to syslog services to setup output entities on a selection of log sources.
Configurable	True

buffer [buffer-name](#) *string*

Context	system logging buffer buffer-name <i>string</i>
Tree	buffer
Description	Log files maintained in memory, non-persistent across system reboots These files are stored at directory <code>/var/log/srlinux/buffer</code> . Rotation into multiple files is available.
Configurable	True

buffer-name *string*

Context	system logging buffer buffer-name <i>string</i>
Description	Base name of the file(s) to be stored in memory
Configurable	True

facility **facility-name** *keyword*

Context	system logging buffer buffer-name <i>string</i> facility facility-name <i>keyword</i>
Tree	facility
Description	List of facilities to source messages from
Configurable	True

facility-name *keyword*

Context	system logging buffer buffer-name <i>string</i> facility facility-name <i>keyword</i>
Description	Name of a Linux syslog facility
Options	<ul style="list-style-type: none">• auth• authpriv• cron• daemon• ftp• kern• lpr• mail• news• syslog• user• uucp• local0• local1• local2• local3• local4• local5• local6• local7
Configurable	True

priority

Context	system logging buffer buffer-name <i>string</i> facility facility-name <i>keyword</i> priority
Tree	priority
Description	Narrows the capture to a given severity, a range or a specific set of severities
Configurable	True

match-above *keyword*

Context	system logging buffer buffer-name <i>string</i> facility facility-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Description	At a given severity and above
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

match-exact *keyword*

Context	system logging buffer buffer-name <i>string</i> facility facility-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Description	Individually specified severities
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

filter *reference*

Context	system logging buffer buffer-name <i>string filter reference</i>
Tree	filter
Description	A set of all-matching criteria that messages must fulfill in order to be captured
Reference	system logging filter filter-name <i>string</i>
Configurable	True

format *string*

Context	system logging buffer buffer-name <i>string format string</i>
Tree	format
Description	Text format of the output syslog messages, in legacy syslog \$template style
Default	%TIMEGENERATED:::date-rfc3339% %HOSTNAME% %SYSLOGTAG%%MSG:::sp-if-no-1st-sp%%MSG:::drop-last-lf%\n
Configurable	True

persist *number*

Context	system logging buffer buffer-name <i>string persist number</i>
Tree	persist
Description	Time in seconds to shadow the buffer to persistent storage Setting this field to 0 results in the buffer not being persisted. A value other than 0 will result in the log being persisted to disk based on the configured value. Logs with a non-zero persist value are persisted automatically on rollover, or at the configured value.
Range	0 60 to 604800
Default	0
Units	seconds
Configurable	True

rotate *number*

Context	system logging buffer buffer-name <i>string rotate number</i>
Tree	rotate
Description	Number of files to keep in rotation when a maximum file size is reached
Default	4
Configurable	True

rotations *number*

Context	system logging buffer buffer-name <i>string rotations number</i>
Tree	rotations
Description	Number of file rotations occurred
Default	0
Configurable	False

size *string*

Context	system logging buffer buffer-name <i>string size string</i>
Tree	size
Description	Number of bytes an individual output file cannot exceed The field allows the 'K, M, or G' suffixes as shorthand. When reaching that size, a rotation happens and subsequent data is stored in a new file with the same base name.
Default	10M
Configurable	True

subsystem **subsystem-name** *keyword*

Context	system logging buffer buffer-name <i>string subsystem subsystem-name keyword</i>
Tree	subsystem
Description	Entity or entities that may produce messages to be captured
Configurable	True

subsystem-name *keyword*

Context	system logging buffer buffer-name <i>string subsystem subsystem-name keyword</i>
Description	Reference to an available subsystem to source messages from
Options	<ul style="list-style-type: none">• aaa• accounting• acl• app• arpd• bfd• bgp• chassis• debug

- dhcp
- fib
- gnmi
- isis
- json
- linux
- lldp
- log
- mgmt
- mpls
- netinst
- platform
- policy
- qos
- sdk
- staticroute
- xdp

Configurable True

priority

Context **system logging buffer buffer-name** *string* **subsystem subsystem-name** *keyword* **priority**

Tree **priority**

Description Narrows the capture to a given severity, a range or a specific set of severities

Configurable True

match-above *keyword*

Context **system logging buffer buffer-name** *string* **subsystem subsystem-name** *keyword* **priority**
match-above *keyword*

Tree **match-above**

Description At a given severity and above

Options

- emergency
- alert
- critical
- error
- warning
- notice
- informational

Configurable

- debug

 True

match-exact *keyword*

Context **system logging buffer buffer-name** *string* **subsystem subsystem-name** *keyword* **priority**
match-exact *keyword*

Tree **match-exact**

Description Individually specified severities

Options

- emergency
- alert
- critical
- error
- warning
- notice
- informational
- debug

Configurable True

console

Context **system logging console**

Tree **console**

Description Hardware serial device normally used for bring-up and diagnostics

Configurable True

facility **facility-name** *keyword*

Context **system logging console facility facility-name** *keyword*

Tree **facility**

Description List of facilities to source messages from

Configurable True

facility-name *keyword*

Context **system logging console facility facility-name** *keyword*

Description Name of a Linux syslog facility

Options

- auth

- authpriv
- cron
- daemon
- ftp
- kern
- lpr
- mail
- news
- syslog
- user
- uucp
- local0
- local1
- local2
- local3
- local4
- local5
- local6
- local7

Configurable True

priority

Context [system logging console facility facility-name](#) *keyword* [priority](#)

Tree [priority](#)

Description Narrows the capture to a given severity, a range or a specific set of severities

Configurable True

match-above *keyword*

Context [system logging console facility facility-name](#) *keyword* [priority match-above](#) *keyword*

Tree [match-above](#)

Description At a given severity and above

- Options
- emergency
 - alert
 - critical
 - error
 - warning
 - notice

- informational
 - debug
- Configurable True

match-exact *keyword*

- Context **system logging console facility facility-name** *keyword* **priority match-exact** *keyword*
- Tree **match-exact**
- Description Individually specified severities
- Options
- emergency
 - alert
 - critical
 - error
 - warning
 - notice
 - informational
 - debug
- Configurable True

filter *reference*

- Context **system logging console filter** *reference*
- Tree **filter**
- Description A set of all-matching criteria that messages must fulfill in order to be captured
- Reference **system logging filter filter-name** *string*
- Configurable True

format *string*

- Context **system logging console format** *string*
- Tree **format**
- Description Text format of the output syslog messages, in legacy syslog \$template style
- Default %TIMEGENERATED::%SYSLOGTAG%%MSG::

Configurable True

subsystem *subsystem-name* *keyword*

Context	system logging console subsystem subsystem-name <i>keyword</i>
Tree	subsystem
Description	Entity or entities that may produce messages to be captured
Configurable	True

subsystem-name *keyword*

Context	system logging console subsystem subsystem-name <i>keyword</i>
Description	Reference to an available subsystem to source messages from
Options	<ul style="list-style-type: none">• aaa• accounting• acl• app• arpd• bfd• bgp• chassis• debug• dhcp• fib• gnmi• isis• json• linux• lldp• log• mgmt• mpls• netinst• platform• policy• qos• sdk• staticroute• xdp
Configurable	True

priority

Context	system logging console subsystem subsystem-name <i>keyword</i> priority
Tree	priority
Description	Narrows the capture to a given severity, a range or a specific set of severities
Configurable	True

match-above *keyword*

Context	system logging console subsystem subsystem-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Description	At a given severity and above
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

match-exact *keyword*

Context	system logging console subsystem subsystem-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Description	Individually specified severities
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

file *file-name string*

Context	system logging file file-name string
Tree	file
Description	Log files maintained on disk, persistent across system reboots When a maximum file size is reached, the file is renamed and a maximum rotate number of them are kept.
Configurable	True

file-name *string*

Context	system logging file file-name string
Description	Base name of the file(s) to be stored on disk
Configurable	True

directory *string*

Context	system logging file file-name string directory string
Tree	directory
Description	Fully qualified path of a directory where the log file(s) shall be maintained
Default	/var/log/srlinux/file
Configurable	True

facility *facility-name keyword*

Context	system logging file file-name string facility facility-name keyword
Tree	facility
Description	List of facilities to source messages from
Configurable	True

facility-name *keyword*

Context	system logging file file-name string facility facility-name keyword
Description	Name of a Linux syslog facility
Options	<ul style="list-style-type: none">• auth• authpriv• cron• daemon• ftp

- kern
- lpr
- mail
- news
- syslog
- user
- uucp
- local0
- local1
- local2
- local3
- local4
- local5
- local6
- local7

Configurable True

priority

Context **system logging file file-name** *string* **facility facility-name** *keyword* **priority**

Tree **priority**

Description Narrows the capture to a given severity, a range or a specific set of severities

Configurable True

match-above *keyword*

Context **system logging file file-name** *string* **facility facility-name** *keyword* **priority match-above** *keyword*

Tree **match-above**

Description At a given severity and above

- Options
- emergency
 - alert
 - critical
 - error
 - warning
 - notice
 - informational
 - debug

Configurable True

match-exact *keyword*

Context	system logging file file-name <i>string</i> facility facility-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Description	Individually specified severities
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

filter *reference*

Context	system logging file file-name <i>string</i> filter <i>reference</i>
Tree	filter
Description	A set of all-matching criteria that messages must fulfill in order to be captured
Reference	system logging filter filter-name <i>string</i>
Configurable	True

format *string*

Context	system logging file file-name <i>string</i> format <i>string</i>
Tree	format
Description	Text format of the output syslog messages, in legacy syslog \$template style
Default	%TIMEGENERATED:: <date-rfc3339% %hostname%<br=""></date-rfc3339%> %SYSLOGTAG%%MSG:: <sp-if-no-1st-sp%%msg::<drop-last-lf%\n< td=""></sp-if-no-1st-sp%%msg::<drop-last-lf%\n<>
Configurable	True

rotate *number*

Context	system logging file file-name <i>string rotate number</i>
Tree	rotate
Description	Number of files to keep in rotation when a maximum file size is reached
Default	4
Configurable	True

rotations *number*

Context	system logging file file-name <i>string rotations number</i>
Tree	rotations
Description	Number of file rotations occurred
Default	0
Configurable	False

size *string*

Context	system logging file file-name <i>string size string</i>
Tree	size
Description	Number of bytes an individual output file cannot exceed The field allows the 'K, M, or G' suffixes as shorthand. When reaching that size, a rotation happens and subsequent data is stored in a new file with the same base name.
Default	10M
Configurable	True

subsystem **subsystem-name** *keyword*

Context	system logging file file-name <i>string subsystem subsystem-name keyword</i>
Tree	subsystem
Description	Entity or entities that may produce messages to be captured
Configurable	True

subsystem-name *keyword*

Context	system logging file file-name <i>string subsystem subsystem-name keyword</i>
Description	Reference to an available subsystem to source messages from
Options	<ul style="list-style-type: none">• aaa

- accounting
- acl
- app
- arpd
- bfd
- bgp
- chassis
- debug
- dhcp
- fib
- gnmi
- isis
- json
- linux
- lldp
- log
- mgmt
- mpls
- netinst
- platform
- policy
- qos
- sdk
- staticroute
- xdp

Configurable True

priority

Context **system logging file file-name** *string* **subsystem subsystem-name** *keyword* **priority**

Tree **priority**

Description Narrows the capture to a given severity, a range or a specific set of severities

Configurable True

match-above *keyword*

Context	system logging file file-name <i>string</i> subsystem subsystem-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Description	At a given severity and above
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

match-exact *keyword*

Context	system logging file file-name <i>string</i> subsystem subsystem-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Description	Individually specified severities
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

filter **filter-name** *string*

Context	system logging filter filter-name <i>string</i>
Tree	filter
Description	Describes a set of criteria that captured messages are required to fulfill
Configurable	True

filter-name *string*

Context	system logging filter filter-name <i>string</i>
Description	Name of the filter
Configurable	True

contains *string*

Context	system logging filter filter-name <i>string</i> contains <i>string</i>
Tree	contains
Description	Text to find in the MSG property of messages to capture from the stream This is slower than prefix.
Configurable	True

facility **facility-name** *keyword*

Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i>
Tree	facility
Description	List of facilities to source messages from
Configurable	True

facility-name *keyword*

Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i>
Description	Name of a Linux syslog facility
Options	<ul style="list-style-type: none">• auth• authpriv• cron• daemon• ftp• kern• lpr• mail• news• syslog• user• uucp• local0• local1

- local2
 - local3
 - local4
 - local5
 - local6
 - local7
- Configurable True

priority

- Context **system logging filter filter-name** *string* **facility facility-name** *keyword* **priority**
- Tree **priority**
- Description Narrows the capture to a given severity, a range or a specific set of severities
- Configurable True

match-above *keyword*

- Context **system logging filter filter-name** *string* **facility facility-name** *keyword* **priority**
match-above *keyword*
- Tree **match-above**
- Description At a given severity and above
- Options
- emergency
 - alert
 - critical
 - error
 - warning
 - notice
 - informational
 - debug
- Configurable True

match-exact *keyword*

- Context **system logging filter filter-name** *string* **facility facility-name** *keyword* **priority**
match-exact *keyword*
- Tree **match-exact**
- Description Individually specified severities
- Options
- emergency

- alert
- critical
- error
- warning
- notice
- informational
- debug

Configurable True

prefix *string*

Context [system logging filter filter-name](#) *string* **prefix** *string*

Tree **prefix**

Description Text to be present at the beginning of the MSG property of a message This is a fast lookup.

Configurable True

regex *string*

Context [system logging filter filter-name](#) *string* **regex** *string*

Tree **regex**

Description Extended regular expression to search in the MSG property of messages

Configurable True

tag *string*

Context [system logging filter filter-name](#) *string* **tag** *string*

Tree **tag**

Description Text to be searched in the SYSLOGTAG property of messages Usually a program name or part of it.

Configurable True

network-instance *reference*

Context [system logging network-instance](#) *reference*

Tree **network-instance**

Description Reference to a configured network-instance to run rsyslogd in

This network-instance will be used as a source for requests to remote syslog servers.

Reference **network-instance name** *string*
Configurable True

remote-server host (*ipv4-address | ipv6-address | domain-name*)

Context **system logging remote-server host** (*ipv4-address | ipv6-address | domain-name*)
Tree **remote-server**
Description List of output remote syslog servers
Configurable True

host (*ipv4-address | ipv6-address | domain-name*)

Context **system logging remote-server host** (*ipv4-address | ipv6-address | domain-name*)
Description Domain or IP address of a remote syslog server destination
String Length 1 to 253
Configurable True

facility facility-name *keyword*

Context **system logging remote-server host** (*ipv4-address | ipv6-address | domain-name*) **facility facility-name** *keyword*
Tree **facility**
Description List of facilities to source messages from
Configurable True

facility-name *keyword*

Context **system logging remote-server host** (*ipv4-address | ipv6-address | domain-name*) **facility facility-name** *keyword*
Description Name of a Linux syslog facility
Options

- auth
- authpriv
- cron
- daemon
- ftp
- kern
- lpr

- mail
- news
- syslog
- user
- uucp
- local0
- local1
- local2
- local3
- local4
- local5
- local6
- local7

Configurable True

priority

Context **system logging remote-server host** (*ipv4-address | ipv6-address | domain-name*) **facility facility-name** *keyword* **priority**

Tree **priority**

Description Narrows the capture to a given severity, a range or a specific set of severities

Configurable True

match-above *keyword*

Context **system logging remote-server host** (*ipv4-address | ipv6-address | domain-name*) **facility facility-name** *keyword* **priority match-above** *keyword*

Tree **match-above**

Description At a given severity and above

- Options
- emergency
 - alert
 - critical
 - error
 - warning
 - notice
 - informational
 - debug

Configurable True

match-exact *keyword*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) facility facility-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Description	Individually specified severities
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

filter *reference*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) filter reference
Tree	filter
Description	A set of all-matching criteria that messages must fulfill in order to be captured
Reference	system logging filter filter-name <i>string</i>
Configurable	True

remote-port *number*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) remote-port <i>number</i>
Tree	remote-port
Description	Transport port for syslog to use for messages sent to a remote server
Default	514
Configurable	True

subsystem *subsystem-name* *keyword*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) subsystem subsystem-name <i>keyword</i>
Tree	subsystem
Description	Entity or entities that may produce messages to be captured
Configurable	True

subsystem-name *keyword*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) subsystem subsystem-name <i>keyword</i>
Description	Reference to an available subsystem to source messages from
Options	<ul style="list-style-type: none">• aaa• accounting• acl• app• arpd• bfd• bgp• chassis• debug• dhcp• fib• gnmi• isis• json• linux• lldp• log• mgmt• mpls• netinst• platform• policy• qos• sdk• staticroute• xdp
Configurable	True

priority

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) subsystem subsystem-name <i>keyword</i> priority
Tree	priority
Description	Narrows the capture to a given severity, a range or a specific set of severities
Configurable	True

match-above *keyword*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) subsystem subsystem-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Description	At a given severity and above
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

match-exact *keyword*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) subsystem subsystem-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Description	Individually specified severities
Options	<ul style="list-style-type: none">• emergency• alert• critical• error• warning• notice• informational• debug
Configurable	True

transport *keyword*

Context	system logging remote-server host (<i>ipv4-address ipv6-address domain-name</i>) transport <i>keyword</i>
Tree	transport
Description	Transport protocol for syslog to use for messages sent to a remote server
Default	udp
Options	<ul style="list-style-type: none">• udp• tcp
Configurable	True

subsystem-facility *keyword*

Context	system logging subsystem-facility <i>keyword</i>
Tree	subsystem-facility
Description	Linux facility that internal application subsystems will use
Default	local6
Options	<ul style="list-style-type: none">• auth• authpriv• cron• daemon• ftp• kern• lpr• mail• news• syslog• user• uucp• local0• local1• local2• local3• local4• local5• local6• local7
Configurable	True

maintenance

Context	system maintenance
Tree	maintenance
Description	Top-level container for Maintenance Mode configuration
Configurable	True

group name *string*

Context	system maintenance group name <i>string</i>
Tree	group
Description	List of user-configured and built-in maintenance groups
Configurable	True

name *string*

Context	system maintenance group name <i>string</i>
Description	Name of the maintenance group. The name "system" is reserved
Configurable	True

maintenance-mode

Context	system maintenance group name <i>string</i> maintenance-mode
Tree	maintenance-mode
Description	Container for activating maintenance mode
Configurable	True

admin-state *keyword*

Context	system maintenance group name <i>string</i> maintenance-mode admin-state <i>keyword</i>
Tree	admin-state
Description	Enable or disable maintenance mode group
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

maintenance-profile *reference*

Context	system maintenance group name <i>string</i> maintenance-profile <i>reference</i>
Tree	maintenance-profile
Description	Leaf reference to /system/maintenance/profile/name
Reference	system maintenance profile name <i>string</i>
Configurable	True

members

Context	system maintenance group name <i>string</i> members
Tree	members
Description	Container for specifying the members of the maintenance group - i.e. the components that will eventually be taken out of service for repair or replacement.
Configurable	True

bgp

Context	system maintenance group name <i>string</i> members bgp
Tree	bgp
Description	Container for specifying the BGP members of the maintenance group
Configurable	True

network-instance **name** *reference*

Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i>
Tree	network-instance
Description	List of network instances with one or more peers to be placed in maintenance mode
Configurable	True

name *reference*

Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i>
Description	A unique name identifying the network instance
Reference	network-instance name <i>string</i>
Configurable	True

neighbor *reference*

Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i> neighbor <i>reference</i>
Tree	neighbor
Description	List of BGP neighbors that belong to the network instance and that should be part of the maintenance group It is not necessary to list neighbors that are members of peer-groups that are already listed. If this list is empty and so is the group list, then the system interprets the meaning as ALL static and dynamic sessions belonging to the specified network-instance.
Reference	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>)
Configurable	True

peer-group *reference*

Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i> peer-group <i>reference</i>
Tree	peer-group
Description	List of BGP peer groups that belong to the network instance and that should be part of the maintenance group If this list is empty and so is the neighbor list, then the system interprets the meaning as ALL static and dynamic sessions belonging to the specified network-instance.
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Configurable	True

profile name *string*

Context	system maintenance profile name <i>string</i>
Tree	profile
Description	
Configurable	True

name *string*

Context	system maintenance profile name <i>string</i>
Description	Name of the maintenance profile
Configurable	True

bgp

Context	system maintenance profile name <i>string</i> bgp
Tree	bgp
Description	Container for BGP policies used to achieve traffic draining
Configurable	True

export-policy *reference*

Context	system maintenance profile name <i>string</i> bgp export-policy <i>reference</i>
Tree	export-policy
Description	
Reference	routing-policy policy name <i>string</i>
Configurable	True

import-policy *reference*

Context	system maintenance profile name <i>string</i> bgp import-policy <i>reference</i>
Tree	import-policy
Description	
Reference	routing-policy policy name <i>string</i>
Configurable	True

mtu

Context	system mtu
Tree	mtu
Description	Top-level container for configuration and state data related to the system MTU
Configurable	True

default-ip-mtu *number*

Context	system mtu default-ip-mtu <i>number</i>
Tree	default-ip-mtu
Description	System default IP MTU in bytes including the IP header but excluding Ethernet overhead
Range	1280 to 9486
Default	1500
Configurable	True

default-l2-mtu *number*



Note: This command is available for the following platforms:

- 7220 IXR-D2
- 7220 IXR-D1
- 7220 IXR-D3

Context	system mtu default-l2-mtu <i>number</i>
Tree	default-l2-mtu
Description	System default Layer-2 MTU in bytes including ethernet overhead and VLAN tags but excluding 4-bytes FCS
Range	1500 to 9500
Default	9232
Configurable	True

default-port-mtu *number*

Context	system mtu default-port-mtu <i>number</i>
Tree	default-port-mtu
Description	System default port MTU in bytes including ethernet overhead but excluding 4-bytes FCS
Range	1500 to 9500
Default	9232
Configurable	True

min-path-mtu *number*

Context	system mtu min-path-mtu <i>number</i>
Tree	min-path-mtu
Description	Sets the minimum path MTU to use when receiving an ICMP fragmentation needed message This is controlled via the kernel min_pmtu option. In the event an ICMP fragmentation needed message is received by the kernel, the system will drop the session to this MTU to allow packets to traverse the entire path.
Range	552 to 9232
Default	552
Configurable	True

name

Context	system name
Tree	name
Description	Contains configuration and state related to system naming
Configurable	True

domain-name *string*

Context	system name domain-name <i>string</i>
Tree	domain-name
Description	The system domain name
String Length	1 to 253
Configurable	True

host-name *string*

Context	system name host-name <i>string</i>
Tree	host-name
Description	The system host name
String Length	1 to 63
Configurable	True

ntp

Context	system ntp
Tree	ntp
Description	Top-level container for NTP configuration and state
Configurable	True

admin-state *keyword*

Context	system ntp admin-state <i>keyword</i>
Tree	admin-state
Description	Enables the system NTP client and indicates that the system should attempt to synchronize the clock
Options	<ul style="list-style-type: none">enable

- disable
- Configurable True

network-instance *reference*

- Context [system ntp network-instance](#) *reference*
- Tree [network-instance](#)
- Description Reference to a configured network-instance
- Reference [network-instance name](#) *string*
- Configurable True

oper-state *keyword*

- Context [system ntp oper-state](#) *keyword*
- Tree [oper-state](#)
- Description Details the operational state of the NTP client
- Options
- up
Component or process is operational
 - down
Component or process is not operational
 - empty
Component slot is empty
 - downloading
Component is downloading image into memory
 - booting
Component is booting downloaded image
 - starting
Component image operational, application processes starting
 - failed
Component or process has failed
 - synchronizing
Component is currently being synchronized
 - upgrading
Component is currently being upgraded
- Configurable False

server address (*ipv4-address | ipv6-address*)

Context	system ntp server address (<i>ipv4-address ipv6-address</i>)
Tree	server
Description	List of NTP servers to use for system clock synchronization
Configurable	True

address (*ipv4-address | ipv6-address*)

Context	system ntp server address (<i>ipv4-address ipv6-address</i>)
Description	IP address of the NTP server, may be either IPv4 or IPv6
Configurable	True

iburst *boolean*

Context	system ntp server address (<i>ipv4-address ipv6-address</i>) iburst <i>boolean</i>
Tree	iburst
Description	Indicates whether this server should enable burst synchronization or not <i>iburst</i> , or initial burst, improves the time taken for initial synchronization by sending a burst of eight packets instead of the usual one, these packets are spaced by a two second delay
Default	false
Configurable	True

jitter *string*

Context	system ntp server address (<i>ipv4-address ipv6-address</i>) jitter <i>string</i>
Tree	jitter
Description	Measurement of the variance in latency on the network
Configurable	False

offset *string*

Context	system ntp server address (<i>ipv4-address ipv6-address</i>) offset <i>string</i>
Tree	offset
Description	Estimate of the current time offset from the peer This is the time difference between the local and reference clock.
Configurable	False

poll-interval *number*

Context	system ntp server address (<i>ipv4-address ipv6-address</i>) poll-interval <i>number</i>
Tree	poll-interval
Description	Polling interval of the peer
Range	16 to 3600
Units	seconds
Configurable	False

prefer *boolean*

Context	system ntp server address (<i>ipv4-address ipv6-address</i>) prefer <i>boolean</i>
Tree	prefer
Description	Indicates whether this server should be preferred or not All other things being equal, this host will be chosen for synchronization among a set of correctly operating NTP servers
Default	false
Configurable	True

stratum *number*

Context	system ntp server address (<i>ipv4-address ipv6-address</i>) stratum <i>number</i>
Tree	stratum
Description	Indicates the level of the server in the NTP hierarchy as number increases, the accuracy is degraded. Primary servers are stratum 1 while a maximum value of 16 indicates unsynchronized. The values have the following meanings: 0 unspecified or invalid 1 primary server (e.g., equipped with a GPS receiver) 2-15 secondary server (via NTP) 16 unsynchronized 17-255 reserved
Configurable	False

synchronized (*ipv4-address | ipv6-address | string*)

Context	system ntp synchronized (<i>ipv4-address ipv6-address string</i>)
Tree	synchronized
Description	Address of the NTP server that the local client is synchronized to This field is set to 'unsynchronized', if the local client is not synchronized
Configurable	False

sflow

Context	system sflow
Tree	sflow
Description	Context to configure sFlow Agent parameters and report sFlow state
Configurable	True

admin-state *keyword*

Context	system sflow admin-state <i>keyword</i>
Tree	admin-state
Description	Administratively enable or disable sFlow for the system
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

collector [collector-id](#) *number*

Context	system sflow collector collector-id <i>number</i>
Tree	collector
Description	List of sFlow collectors to which sFlow sample data is sent
Configurable	True
Max. Elements	8

collector-id *number*

Context	system sflow collector collector-id <i>number</i>
Description	Specify the collector ID
Range	1 to 8
Configurable	True

collector-address (*ipv4-address | ipv6-address*)

Context	system sflow collector collector-id <i>number</i> collector-address (<i>ipv4-address ipv6-address</i>)
Tree	collector-address
Description	The IP address for an sFlow collector
Configurable	True

network-instance *reference*

Context	system sflow collector collector-id <i>number</i> network-instance <i>reference</i>
Tree	network-instance
Description	Reference to a configured network-instance
Reference	network-instance name <i>string</i>
Configurable	True

next-hop (*ipv4-address | ipv6-address*)

Context	system sflow collector collector-id <i>number</i> next-hop (<i>ipv4-address ipv6-address</i>)
Tree	next-hop
Description	Specifies the active IP next hop used to reach the associated collector
Configurable	False

port *number*

Context	system sflow collector collector-id <i>number</i> port <i>number</i>
Tree	port
Description	Specifies the destination UDP port number to be used in sFlow packets
Default	6343
Configurable	True

source-address (*ipv4-address | ipv6-address*)

Context	system sflow collector collector-id <i>number</i> source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Description	Specifies the IP address to be used as the source address in sFlow packets
Configurable	True

sample-rate *number*

Context	system sflow sample-rate <i>number</i>
Tree	sample-rate
Description	Specify sFlow sample rate This value is the rate at which traffic will be sampled at a rate of 1:N received packets.
Range	1 to 2000000
Default	10000
Configurable	True

sample-size *number*

Context	system sflow sample-size <i>number</i>
Tree	sample-size
Description	Specify sFlow sample size This value specifies the number of bytes the sFlow agent samples from each frame.
Range	256
Default	256
Configurable	True

statistics

Context	system sflow statistics
Tree	statistics
Description	
Configurable	False

total-offered-packets *number*

Context	system sflow statistics total-offered-packets <i>number</i>
Tree	total-offered-packets
Description	Total number of packets subject to sFlow sampling
Default	0
Configurable	False

total-samples-taken *number*

Context	system sflow statistics total-samples-taken <i>number</i>
Tree	total-samples-taken
Description	Total number of sFlow samples taken
Default	0
Configurable	False

total-sent-packets *number*

Context	system sflow statistics total-sent-packets <i>number</i>
Tree	total-sent-packets
Description	Total number of sFlow packets sent to collectors
Default	0
Configurable	False

snmp

Context	system snmp
Tree	snmp
Description	Top-level container for SNMP configuration and state
Configurable	True

community *string*

Context	system snmp community <i>string</i>
Tree	community
Description	
String Length	1 to 255
Configurable	True

network-instance [name](#) *reference*

Context	system snmp network-instance name <i>reference</i>
Tree	network-instance
Description	List of network-instances to run an SNMP server in
Configurable	True

name *reference*

Context	system snmp network-instance name <i>reference</i>
Description	Reference to a configured network-instance
Reference	network-instance name <i>string</i>
Configurable	True

admin-state *keyword*

Context	system snmp network-instance name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Description	Enables the SNMP server in this network-instance
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system snmp network-instance name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
Description	Details the operational state of the SNMP server
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading

Component is currently being upgraded

Configurable False

source-address (*ipv4-address | ipv6-address*)

Context [system snmp network-instance name](#) *reference* [source-address](#) (*ipv4-address | ipv6-address*)

Tree [source-address](#)

Description List of IP addresses for the SNMP server to listen on within the network-instance

Default ::

Configurable True

ssh-server

Context [system ssh-server](#)

Tree [ssh-server](#)

Description Top-level container for SSH server configuration and state

Configurable True

network-instance name *reference*

Context [system ssh-server network-instance name](#) *reference*

Tree [network-instance](#)

Description List of network-instances to run an SSH server in

Configurable True

name *reference*

Context [system ssh-server network-instance name](#) *reference*

Description Reference to a configured network-instance

Reference [network-instance name](#) *string*

Configurable True

admin-state *keyword*

Context	system ssh-server network-instance name <i>reference admin-state keyword</i>
Tree	admin-state
Description	Enables the SSH server in this network-instance
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True

oper-state *keyword*

Context	system ssh-server network-instance name <i>reference oper-state keyword</i>
Tree	oper-state
Description	Details the operational state of the SSH server
Options	<ul style="list-style-type: none">• up Component or process is operational• down Component or process is not operational• empty Component slot is empty• downloading Component is downloading image into memory• booting Component is booting downloaded image• starting Component image operational, application processes starting• failed Component or process has failed• synchronizing Component is currently being synchronized• upgrading Component is currently being upgraded
Configurable	False

protocol-version *number*

Context	system ssh-server network-instance name <i>reference</i> protocol-version <i>number</i>
Tree	protocol-version
Description	Protocol version in use by the SSH server
Configurable	False

rate-limit *number*

Context	system ssh-server network-instance name <i>reference</i> rate-limit <i>number</i>
Tree	rate-limit
Description	Set a limit on the number of unauthenticated sessions to the SSH server after this number is met, the server will start dropping connection attempts
Default	20
Configurable	True

source-address (*ipv4-address | ipv6-address*)

Context	system ssh-server network-instance name <i>reference</i> source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Description	List of IP addresses for the SSH server to listen on within the network-instance
Configurable	True

timeout *number*

Context	system ssh-server network-instance name <i>reference</i> timeout <i>number</i>
Tree	timeout
Description	Set the idle timeout in seconds on SSH connections
Default	0
Units	seconds
Configurable	True

tls

Context	system tls
Tree	tls
Description	Top-level container for TLS configuration and state
Configurable	True

server-profile *name string*

Context	system tls server-profile name <i>string</i>
Tree	server-profile
Description	List of configured TLS server profiles
Configurable	True

name *string*

Context	system tls server-profile name <i>string</i>
Description	Name of the TLS server-profile
String Length	1 to 255
Configurable	True

authenticate-client *boolean*

Context	system tls server-profile name <i>string</i> authenticate-client <i>boolean</i>
Tree	authenticate-client
Description	Defines if the server should authenticate the identity of connecting clients using the trust anchor
Default	false
Configurable	True

certificate *string*

Context	system tls server-profile name <i>string</i> certificate <i>string</i>
Tree	certificate
Description	Base64 encoded certificate to use with the private key this includes the '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' header and footer
Configurable	True

cipher-list *identityref*

Context	system tls server-profile name <i>string</i> cipher-list <i>identityref</i>
Tree	cipher-list
Description	List of ciphers to use when negotiating TLS with clients
Options	<ul style="list-style-type: none">• ecdhe-rsa-aes256-gcm-sha384• ecdhe-ecdsa-aes256-gcm-sha384• ecdhe-rsa-aes256-sha384• ecdhe-ecdsa-aes256-sha384• ecdhe-rsa-aes256-sha• ecdhe-ecdsa-aes256-sha• dh-dss-aes256-gcm-sha384• dhe-dss-aes256-gcm-sha384• dh-rsa-aes256-gcm-sha384• dhe-rsa-aes256-gcm-sha384• dhe-rsa-aes256-sha256• dhe-dss-aes256-sha256• dh-rsa-aes256-sha256• dh-dss-aes256-sha256• dhe-rsa-aes256-sha• dhe-dss-aes256-sha• dh-rsa-aes256-sha• dh-dss-aes256-sha• dhe-rsa-camellia256-sha• dhe-dss-camellia256-sha• dh-rsa-camellia256-sha• dh-dss-camellia256-sha• ecdh-rsa-aes256-gcm-sha384• ecdh-ecdsa-aes256-gcm-sha384• ecdh-rsa-aes256-sha384• ecdh-ecdsa-aes256-sha384• ecdh-rsa-aes256-sha• ecdh-ecdsa-aes256-sha• aes256-gcm-sha384• aes256-sha256• aes256-sha• camellia256-sha• psk-aes256-cbc-sha• ecdhe-rsa-aes128-gcm-sha256• ecdhe-ecdsa-aes128-gcm-sha256

-
- ecdhe-rsa-aes128-sha256
 - ecdhe-ecdsa-aes128-sha256
 - ecdhe-rsa-aes128-sha
 - ecdhe-ecdsa-aes128-sha
 - dh-dss-aes128-gcm-sha256
 - dhe-dss-aes128-gcm-sha256
 - dh-rsa-aes128-gcm-sha256
 - dhe-rsa-aes128-gcm-sha256
 - dhe-rsa-aes128-sha256
 - dhe-dss-aes128-sha256
 - dh-rsa-aes128-sha256
 - dh-dss-aes128-sha256
 - dhe-rsa-aes128-sha
 - dhe-dss-aes128-sha
 - dh-rsa-aes128-sha
 - dh-dss-aes128-sha
 - dhe-rsa-seed-sha
 - dhe-dss-seed-sha
 - dh-rsa-seed-sha
 - dh-dss-seed-sha
 - dhe-rsa-camellia128-sha
 - dhe-dss-camellia128-sha
 - dh-rsa-camellia128-sha
 - dh-dss-camellia128-sha
 - ecdh-rsa-aes128-gcm-sha256
 - ecdh-ecdsa-aes128-gcm-sha256
 - ecdh-rsa-aes128-sha256
 - ecdh-ecdsa-aes128-sha256
 - ecdh-rsa-aes128-sha
 - ecdh-ecdsa-aes128-sha
 - aes128-gcm-sha256
 - aes128-sha256
 - aes128-sha
 - seed-sha
 - camellia128-sha
 - psk-aes128-cbc-sha
 - ecdhe-rsa-des-cbc3-sha
 - ecdhe-ecdsa-des-cbc3-sha
 - edh-rsa-des-cbc3-sha

- edh-dss-des-cbc3-sha
- dh-rsa-des-cbc3-sha
- dh-dss-des-cbc3-sha
- ecdh-rsa-des-cbc3-sha
- ecdh-ecdsa-des-cbc3-sha
- des-cbc3-sha
- idea-cbc-sha
- psk-3des-ede-cbc-sha
- krb5-idea-cbc-sha
- krb5-des-cbc3-sha
- krb5-idea-cbc-md5
- krb5-des-cbc3-md5
- ecdhe-rsa-rc4-sha
- ecdhe-ecdsa-rc4-sha
- ecdh-rsa-rc4-sha
- ecdh-ecdsa-rc4-sha
- rc4-sha
- rc4-md5
- psk-rc4-sha
- krb5-rc4-sha
- krb5-rc4-md5

Configurable True

key string

Context **system tls server-profile name** string **key** string

Tree **key**

Description Base64 encoded key to use with the server certificate

This includes the '-----BEGIN PRIVATE KEY-----', and '-----END PRIVATE KEY-----' header and footer The value is hashed, and only the hashed value is kept

Configurable True

trust-anchor string

Context **system tls server-profile name** string **trust-anchor** string

Tree **trust-anchor**

Description Base64 encoded certificate to use as a trust anchor This includes the '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' header and footer

Configurable True

trace-options *keyword*

Context	system trace-options <i>keyword</i>
Tree	trace-options
Description	Management server trace options
Options	<ul style="list-style-type: none">• request• response• common
Configurable	True
Introduced	19.11.1

10 tools acl

acl

- + **cpm-filter**
- + **ipv4-filter**
 - + **clear**
 - + **entry sequence-id** *number*
 - + **statistics**
 - + **clear**
- + **ipv6-filter**
 - + **clear**
 - + **entry sequence-id** *number*
 - + **statistics**
 - + **clear**
- + **ipv4-filter name** *string*
 - + **entry sequence-id** *number*
 - + **statistics**
 - + **clear**
 - + **per-interface**
 - + **subinterface name** *string*
 - + **clear**
 - + **statistics**
 - + **clear**
- + **ipv6-filter name** *string*
 - + **entry sequence-id** *number*
 - + **statistics**
 - + **clear**
 - + **per-interface**
 - + **subinterface name** *string*
 - + **clear**
 - + **statistics**
 - + **clear**
- + **policers**
 - + **policer name** *string*
 - + **statistics**
 - + **clear**
 - + **system-cpu-policer name** *string*
 - + **statistics**
 - + **clear**

10.1 acl Descriptions

acl

Context	acl
Tree	acl
Description	Top level enclosing container for ACL operational tools
Configurable	True

cpm-filter

Context	acl cpm-filter
Tree	cpm-filter
Description	List of CPM filters
Configurable	True

ipv4-filter

Context	acl cpm-filter ipv4-filter
Tree	ipv4-filter
Description	List of CPM IPv4 filter rules
Configurable	True

clear

Context	acl cpm-filter ipv4-filter clear
Tree	clear
Description	Reset all statistics of all entries of the filter to zero
Configurable	True

entry [sequence-id](#) *number*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Configurable	True

statistics

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics clear
Tree	clear
Description	Reset all statistics associated with this particular entry to zero
Configurable	True

ipv6-filter

Context	acl cpm-filter ipv6-filter
Tree	ipv6-filter
Description	List of CPM IPv6 filter rules
Configurable	True

clear

Context	acl cpm-filter ipv6-filter clear
Tree	clear
Description	Reset all statistics of all entries of the filter to zero
Configurable	True

entry **sequence-id** *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Configurable	True

statistics

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics clear
Tree	clear
Description	Reset all statistics associated with this particular entry to zero
Configurable	True

ipv4-filter **name** *string*

Context	acl ipv4-filter name <i>string</i>
Tree	ipv4-filter
Description	List of IPv4 filter policies
Configurable	True

name *string*

Context	acl ipv4-filter name <i>string</i>
Description	Name of the IPv4 filter policy.
String Length	1 to 255
Configurable	True

entry **sequence-id** *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Configurable	True

statistics

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics clear
Tree	clear
Description	Reset all aggregate and per-interface statistics associated with this particular entry to zero
Configurable	True

per-interface

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Description	Container for per-subinterface per-entry statistics
Configurable	True

subinterface *name string*

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Description	List of subinterfaces where the ACL is applied to either input or output traffic
Configurable	True

name string

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Description	
String Length	3 to 24
Configurable	True

clear

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> clear
Tree	clear
Description	Reset the per-interface statistics associated with this particular entry and this particular subinterface to zero
Configurable	True

statistics

Context	acl ipv4-filter name <i>string</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl ipv4-filter name <i>string</i> statistics clear
Tree	clear
Description	Reset all statistics of all entries of the filter to zero
Configurable	True

ipv6-filter name *string*

Context	acl ipv6-filter name <i>string</i>
Tree	ipv6-filter
Description	List of IPv6 filter policies
Configurable	True

name *string*

Context	acl ipv6-filter name <i>string</i>
Description	Name of the IPv6 filter policy.
String Length	1 to 255
Configurable	True

entry **sequence-id** *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Tree	entry
Description	List of filter rules.
Configurable	True

sequence-id *number*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Configurable	True

statistics

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics clear
Tree	clear
Description	Reset all aggregate and per-interface statistics associated with this particular entry to zero
Configurable	True

per-interface

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Description	Container for per-subinterface per-entry statistics
Configurable	True

subinterface name *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Description	List of subinterfaces where the ACL is applied to either input or output traffic
Configurable	True

name *string*

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Description	
String Length	3 to 24
Configurable	True

clear

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i> clear
Tree	clear
Description	Reset the per-interface statistics associated with this particular entry and this particular subinterface to zero
Configurable	True

statistics

Context	acl ipv6-filter name <i>string</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl ipv6-filter name <i>string</i> statistics clear
Tree	clear
Description	Reset all statistics of all entries of the filter to zero
Configurable	True

policers

Context	acl policers
Tree	policers
Description	List of policers used by ACL entries
Configurable	True

policer name *string*

Context	acl policers policer name <i>string</i>
Tree	policer
Description	List of hardware policers
Configurable	True

name *string*

Context	acl policers policer name <i>string</i>
Description	Name of the hardware policer
String Length	1 to 255
Configurable	True

statistics

Context	acl policers policer name <i>string</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl policers policer name <i>string</i> statistics clear
Tree	clear
Description	Reset all statistics associated with this particular policer to zero
Configurable	True

system-cpu-policer [name](#) *string*

Context	acl policers system-cpu-policer name <i>string</i>
Tree	system-cpu-policer
Description	List of system CPU policers
Configurable	True

name *string*

Context	acl policers system-cpu-policer name <i>string</i>
Description	Name of the system cpu policer
String Length	1 to 255
Configurable	True

statistics

Context	acl policers system-cpu-policer name <i>string</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	acl policers system-cpu-policer name <i>string</i> statistics clear
Tree	clear
Description	Reset all statistics associated with this particular policer to zero
Configurable	True

11 tools bfd

bfd

- + **peer local-discriminator** *number*
- + **clear**
- + **statistics**
- + **peer local-discriminator** *number*
- + **clear**

11.1 bfd Descriptions

bfd

Context	bfd
Tree	bfd
Description	Top-level grouping for bfd operational commands
Configurable	True

peer [local-discriminator](#) *number*

Context	bfd peer local-discriminator <i>number</i>
Tree	peer
Description	The list of local-discriminators associated with BFD
Configurable	True

local-discriminator *number*

Context	bfd peer local-discriminator <i>number</i>
Description	BFD session local discriminator
Configurable	True

clear

Context	bfd peer local-discriminator <i>number</i> clear
Tree	clear
Description	Clear the associated BFD sessions Clearing a BFD sessions causes the associated BFD sessions ot transition to a Down satate
Configurable	True

statistics

Context	bfd statistics
Tree	statistics
Description	
Configurable	True

peer local-discriminator *number*

Context	bfd statistics peer local-discriminator <i>number</i>
Tree	peer
Description	The list of local-discriminators associated with BFD
Configurable	True

local-discriminator *number*

Context	bfd statistics peer local-discriminator <i>number</i>
Description	BFD session local discriminator
Configurable	True

clear

Context	bfd statistics peer local-discriminator <i>number</i> clear
Tree	clear
Description	Clear the BFD statistics associated the the BFD sessions
Configurable	True

12 tools interface

```
interface name string
+ ethernet
+   statistics
+     clear
+ statistics
+   clear
+   queue-statistics
+     clear
+     multicast-queue queue-id number
+       clear
+     unicast-queue queue-id number
+       clear
+ subinterface index number
+   bridge-table
+     mac-duplication
+       delete-all-macs
+       delete-mac address string
+     mac-learning
+       delete-all-macs
+       delete-mac address string
+   ipv4
+     arp
+       delete-dynamic
+       neighbor ipv4-address string
+         delete-dynamic
+   ipv6
+     neighbor-discovery
+       delete-dynamic
+       neighbor ipv6-address string
+         delete-dynamic
+   statistics
+     clear
```

12.1 interface Descriptions

interface **name** *string*

Context	interface name <i>string</i>
Tree	interface
Description	The list of named interfaces on the device.
Configurable	True

name *string*

Context	interface name <i>string</i>
Description	References the configured name of the interface
Configurable	True

ethernet

Context	interface name <i>string</i> ethernet
Tree	ethernet
Description	
Configurable	True

statistics

Context	interface name <i>string</i> ethernet statistics
Tree	statistics
Description	
Configurable	True

clear

Context	interface name <i>string</i> ethernet statistics clear
Tree	clear
Description	
Configurable	True

statistics

Context	interface name <i>string</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	interface name <i>string</i> statistics clear
Tree	clear
Description	
Configurable	True

queue-statistics

Context	interface name <i>string</i> statistics queue-statistics
Tree	queue-statistics
Description	
Configurable	True

clear

Context	interface name <i>string</i> statistics queue-statistics clear
Tree	clear
Description	
Configurable	True

multicast-queue **queue-id** *number*

Context	interface name <i>string</i> statistics queue-statistics multicast-queue queue-id <i>number</i>
Tree	multicast-queue
Description	
Configurable	True

queue-id *number*

Context	interface name <i>string</i> statistics queue-statistics multicast-queue queue-id <i>number</i>
Description	Queue number: 0-7
Range	0 to 7
Configurable	True

clear

Context	interface name <i>string</i> statistics queue-statistics multicast-queue queue-id <i>number</i> clear
Tree	clear
Description	
Configurable	True

unicast-queue **queue-id** *number*

Context	interface name <i>string</i> statistics queue-statistics unicast-queue queue-id <i>number</i>
Tree	unicast-queue
Description	
Configurable	True

queue-id *number*

Context	interface name <i>string</i> statistics queue-statistics unicast-queue queue-id <i>number</i>
Description	Queue number: 0-7
Range	0 to 7
Configurable	True

clear

Context	interface name <i>string</i> statistics queue-statistics unicast-queue queue-id <i>number</i> clear
Tree	clear
Description	
Configurable	True

subinterface **index** *number*

Context	interface name <i>string</i> subinterface index <i>number</i>
Tree	subinterface
Description	The list of subinterfaces (logical interfaces) associated with a physical interface
Configurable	True

index *number*

Context	interface name <i>string</i> subinterface index <i>number</i>
Description	The index of the subinterface, or logical interface number
Configurable	True

bridge-table

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table
Tree	bridge-table
Description	
Configurable	True

mac-duplication

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication
Tree	mac-duplication
Description	
Configurable	True

delete-all-macs

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication delete-all-macs
Tree	delete-all-macs
Description	Delete all learnt mac entries.
Configurable	True

delete-mac address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication delete-mac address <i>string</i>
Tree	delete-mac
Description	learnt mac address entry to be deleted.
Configurable	True

address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication delete-mac address <i>string</i>
Description	
Configurable	True

mac-learning

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning
Tree	mac-learning
Description	
Configurable	True

delete-all-macs

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning delete-all-macs
Tree	delete-all-macs
Description	Delete all learnt mac entries.
Configurable	True

delete-mac address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning delete-mac address <i>string</i>
Tree	delete-mac
Description	learnt mac address entry to be deleted.
Configurable	True

address *string*

Context **interface name** *string* **subinterface index** *number* **bridge-table mac-learning delete-mac address** *string*

Description

Configurable True

ipv4

Context **interface name** *string* **subinterface index** *number* **ipv4**

Tree **ipv4**

Description

Configurable True

arp

Context **interface name** *string* **subinterface index** *number* **ipv4 arp**

Tree **arp**

Description

Configurable True

delete-dynamic

Context **interface name** *string* **subinterface index** *number* **ipv4 arp delete-dynamic**

Tree **delete-dynamic**

Description Delete all dynamic ARP entries

Configurable True

neighbor **ipv4-address** *string*

Context **interface name** *string* **subinterface index** *number* **ipv4 arp neighbor ipv4-address** *string*

Tree **neighbor**

Description

Configurable True

ipv4-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>
Description	IPv4 address resolved by the ARP entry
Configurable	True

delete-dynamic

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> delete-dynamic
Tree	delete-dynamic
Description	Delete one specific dynamic ARP entry
Configurable	True

ipv6

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6
Tree	ipv6
Description	
Configurable	True

neighbor-discovery

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery
Tree	neighbor-discovery
Description	
Configurable	True

delete-dynamic

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery delete-dynamic
Tree	delete-dynamic
Description	Delete all dynamic neighbor cache entries
Configurable	True

neighbor **ipv6-address** *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Tree	neighbor
Description	
Configurable	True

ipv6-address *string*

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Description	IPv6 address resolved by the ND cache entry
Configurable	True

delete-dynamic

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> delete-dynamic
Tree	delete-dynamic
Description	Delete one specific dynamic neighbor cache entry
Configurable	True

statistics

Context	interface name <i>string</i> subinterface index <i>number</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	interface name <i>string</i> subinterface index <i>number</i> statistics clear
Tree	clear
Description	
Configurable	True

13 tools network-instance

network-instance *name* *string*

- + **bridge-table**
 - + **mac-duplication**
 - + **delete-mac** *address* *string*
 - + **delete-macs-type** *keyword*
 - + **mac-learning**
 - + **delete-all-macs**
 - + **delete-mac** *address* *string*
- + **icmp**
 - + **statistics**
 - + **clear**
- + **icmp6**
 - + **statistics**
 - + **clear**
- + **protocols**
 - + **bgp**
 - + **group** *group-name* *string*
 - + **reset-peer**
 - + **peer-as** *number*
 - + **soft-clear**
 - + **peer-as** *number*
 - + **route-refresh** *keyword*
 - + **neighbor** *peer-address* (*ipv4-address* | *ipv6-address*)
 - + **reset-peer**
 - + **soft-clear**
 - + **route-refresh** *keyword*
 - + **reset-peer**
 - + **peer-as** *number*
 - + **soft-clear**
 - + **peer-as** *number*
 - + **route-refresh** *keyword*
 - + **isis**
 - + **instance** *name* *string*
 - + **interface** *interface-name* *string*
 - + **adjacencies**
 - + **clear**
 - + **link-state-database**
 - + **clear**
 - + **statistics**
 - + **clear**

13.1 network-instance Descriptions

network-instance **name** *string*

Context **network-instance name** *string*

Tree **network-instance**

Description

Configurable True

name *string*

Context **network-instance name** *string*

Description A unique name identifying the network instance

Configurable True

bridge-table

Context **network-instance name** *string* **bridge-table**

Tree **bridge-table**

Description bridge-table

Configurable True

mac-duplication

Context **network-instance name** *string* **bridge-table mac-duplication**

Tree **mac-duplication**

Description

Configurable True

delete-mac **address** *string*

Context **network-instance name** *string* **bridge-table mac-duplication delete-mac address** *string*

Tree **delete-mac**

Description duplicate mac address entry to be deleted.

Configurable True

address *string*

Context	network-instance name <i>string</i> bridge-table mac-duplication delete-mac address <i>string</i>
Description	
Configurable	True

delete-macs-type *keyword*

Context	network-instance name <i>string</i> bridge-table mac-duplication delete-macs-type <i>keyword</i>
Tree	delete-macs-type
Description	Type of duplicate mac entries to delete
Options	<ul style="list-style-type: none">• all• blackhole-only
Configurable	True

mac-learning

Context	network-instance name <i>string</i> bridge-table mac-learning
Tree	mac-learning
Description	
Configurable	True

delete-all-macs

Context	network-instance name <i>string</i> bridge-table mac-learning delete-all-macs
Tree	delete-all-macs
Description	Delete all learnt mac entries.
Configurable	True

delete-mac [address](#) *string*

Context	network-instance name <i>string</i> bridge-table mac-learning delete-mac address <i>string</i>
Tree	delete-mac
Description	learnt mac address entry to be deleted.
Configurable	True

address *string*

Context	network-instance name <i>string</i> bridge-table mac-learning delete-mac address <i>string</i>
Description	
Configurable	True

icmp

Context	network-instance name <i>string</i> icmp
Tree	icmp
Description	
Configurable	True

statistics

Context	network-instance name <i>string</i> icmp statistics
Tree	statistics
Description	ICMP version 4 statistics
Configurable	True

clear

Context	network-instance name <i>string</i> icmp statistics clear
Tree	clear
Description	Resets all the YANG state counters under network-instance/icmp/statistics to zero
Configurable	True

icmp6

Context	network-instance name <i>string</i> icmp6
Tree	icmp6
Description	
Configurable	True

statistics

Context	network-instance name <i>string</i> icmp6 statistics
Tree	statistics
Description	ICMP version 6 statistics
Configurable	True

clear

Context	network-instance name <i>string</i> icmp6 statistics clear
Tree	clear
Description	Resets all the YANG state counters under network-instance/icmp6/statistics to zero
Configurable	True

protocols

Context	network-instance name <i>string</i> protocols
Tree	protocols
Description	The routing protocols that are enabled for this network-instance.
Configurable	True

bgp

Context	network-instance name <i>string</i> protocols bgp
Tree	bgp
Description	
Configurable	True

group [group-name](#) *string*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Tree	group
Description	
Configurable	True

group-name *string*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Description	The configured name of the peer group
String Length	1 to 255
Configurable	True

reset-peer

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> reset-peer
Tree	reset-peer
Description	
Configurable	True

peer-as *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> reset-peer peer-as <i>number</i>
Tree	peer-as
Description	Hard reset only BGP peers in the peer-group that have the specified peer-AS number, whether they are configured peers or dynamic peers
Range	1 to 4294967295
Configurable	True

soft-clear

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> soft-clear
Tree	soft-clear
Description	
Configurable	True

peer-as *number*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> soft-clear peer-as <i>number</i>
Tree	peer-as
Description	Soft reset only BGP peers in the peer-group that have the specified peer-AS number, whether they are configured peers or dynamic peers
Range	1 to 4294967295
Configurable	True

route-refresh *keyword*

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> soft-clear route-refresh <i>keyword</i>
Tree	route-refresh
Description	The address family to refresh This is encoded in the ROUTE_REFRESH message. By default all families are refreshed.
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	True

neighbor peer-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>)
Tree	neighbor
Description	
Configurable	True

peer-address (*ipv4-address | ipv6-address*)

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>)
Description	The transport address of the BGP peer The peer-address must be a valid IPv4 unicast address or a valid IPv6 global unicast address. Sessions to a link-local IPv6 address are not supported.
Configurable	True

reset-peer

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) reset-peer
Tree	reset-peer
Description	Hard reset the peer
Configurable	True

soft-clear

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) soft-clear
Tree	soft-clear
Description	
Configurable	True

route-refresh *keyword*

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address</i>) soft-clear route-refresh <i>keyword</i>
Tree	route-refresh
Description	The address family to refresh This is encoded in the ROUTE_REFRESH message. By default all families are refreshed.
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	True

reset-peer

Context	network-instance name <i>string</i> protocols bgp reset-peer
Tree	reset-peer
Description	
Configurable	True

peer-as *number*

Context	network-instance name <i>string</i> protocols bgp reset-peer peer-as <i>number</i>
Tree	peer-as
Description	Hard reset only BGP peers that have the specified peer-AS number, whether they are configured peers or dynamic peers
Range	1 to 4294967295
Configurable	True

soft-clear

Context	network-instance name <i>string</i> protocols bgp soft-clear
Tree	soft-clear
Description	
Configurable	True

peer-as *number*

Context	network-instance name <i>string</i> protocols bgp soft-clear peer-as <i>number</i>
Tree	peer-as
Description	Soft reset only BGP peers that have the specified peer-AS number, whether they are configured peers or dynamic peers
Range	1 to 4294967295
Configurable	True

route-refresh *keyword*

Context	network-instance name <i>string</i> protocols bgp soft-clear route-refresh <i>keyword</i>
Tree	route-refresh
Description	The address family to refresh This is encoded in the ROUTE_REFRESH message. By default all families are refreshed.
Options	<ul style="list-style-type: none">• ipv4-unicast• ipv6-unicast
Configurable	True

isis

Context	network-instance name <i>string</i> protocols isis
Tree	isis
Description	
Configurable	True

instance name *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>
Tree	instance
Description	List of IS-IS protocol instances associated with this network-instance. Only a single instance is supported for now
Configurable	True
Max. Elements	1

name *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>
Description	The name of the IS-IS instance
String Length	1 to 255
Configurable	True

interface [interface-name](#) *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>string</i>
Tree	interface
Description	List of IS-IS interfaces
Configurable	True

interface-name *string*

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>string</i>
Description	Reference to a specific subinterface of the form <interface-name>.<subinterface-index>
String Length	3 to 24
Configurable	True

adjacencies

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>string</i> adjacencies
Tree	adjacencies
Description	
Configurable	True

clear

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>string</i> adjacencies clear
Tree	clear
Description	Reset all of the adjacencies on this interface
Configurable	True

link-state-database

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> link-state-database
Tree	link-state-database
Description	The ISIS link state database
Configurable	True

clear

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> link-state-database clear
Tree	clear
Description	Clear the contents of the LSDB.
Configurable	True

statistics

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics
Tree	statistics
Description	
Configurable	True

clear

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics clear
Tree	clear
Description	Reset all of the IS-IS instance statistics to zero.
Configurable	True

14 tools platform

platform

- + chassis
 - + reboot
 - + force
- + control slot *string*
 - + locator
 - + disable
 - + enable
 - + duration *number*
 - + reboot
 - + force
- + fabric slot *number*
 - + locator
 - + disable
 - + enable
 - + duration *number*
 - + reboot
- + fan-tray id *number*
 - + locator
 - + disable
 - + enable
 - + duration *number*
- + linecard slot *number*
 - + locator
 - + disable
 - + enable
 - + duration *number*
 - + reboot
- + redundancy
 - + switchover
 - + synchronize
 - + overlay
 - + system
- + show-fabric-bandwidth

14.1 platform Descriptions

platform

Context	platform
Tree	platform
Description	Top-level container for platform operational commands
Configurable	True

chassis

Context	platform chassis
Tree	chassis
Description	Operational commands related to the chassis
Configurable	True

reboot

Context	platform chassis reboot
Tree	reboot
Description	Trigger a reboot of the chassis
Configurable	True

force

Context	platform chassis reboot force
Tree	force
Description	Force a reboot of the chassis, overriding any synchronizations or other activities in progress This option can be dangerous, and may result in a standby module booting on an older image if used after an image change
Configurable	True

control slot *string*

Context	platform control slot <i>string</i>
Tree	control
Description	Operational commands related to control modules
Configurable	True

slot *string*

Context	platform control slot <i>string</i>
Description	Slot identifier for the control module
Configurable	True

locator

Context	platform control slot <i>string</i> locator
Tree	locator
Description	Operational commands for the locator LED
Configurable	True

disable

Context	platform control slot <i>string</i> locator disable
Tree	disable
Description	Deactivates the locator LED for this component
Configurable	True

enable

Context	platform control slot <i>string</i> locator enable
Tree	enable
Description	Activate the locator LED for this component
Configurable	True

duration *number*

Context	platform control slot <i>string</i> locator enable duration <i>number</i>
Tree	duration
Description	Sets the duration to activate the locator LED, after which it will disable automatically
Range	10 to 3600
Units	seconds
Configurable	True

reboot



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform control slot <i>string</i> reboot
Tree	reboot
Description	Trigger a reboot of the control module
Configurable	True

force



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform control slot <i>string</i> reboot force
Tree	force
Description	Force a reboot of the control module, overriding any synchronizations or other activities in progress This option can be dangerous, and may result in a standby module booting on an older image if used after an image change
Configurable	True

fabric slot number



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number
Tree	fabric
Description	Operational commands related to fabric modules
Configurable	True

slot number



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number
Description	Numeric identifier for the fabric module
Configurable	True

locator



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number locator
Tree	locator
Description	Operational commands for the locator LED
Configurable	True

disable



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number locator disable
Tree	disable
Description	Deactivates the locator LED for this component
Configurable	True

enable



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number locator enable
Tree	enable
Description	Activate the locator LED for this component
Configurable	True

duration *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number locator enable duration number
Tree	duration
Description	Sets the duration to activate the locator LED, after which it will disable automatically
Range	10 to 3600
Units	seconds
Configurable	True

reboot



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform fabric slot number reboot
Tree	reboot
Description	Reboot this component
Configurable	True

fan-tray id number

Context	platform fan-tray id number
Tree	fan-tray
Description	Operational commands related to fan modules
Configurable	True

id number

Context	platform fan-tray id number
Description	Numeric identifier for the fan module
Configurable	True

locator

Context	platform fan-tray id number locator
Tree	locator
Description	Operational commands for the locator LED
Configurable	True

disable

Context	platform fan-tray id number locator disable
Tree	disable
Description	Deactivates the locator LED for this component
Configurable	True

enable

Context	platform fan-tray id number locator enable
Tree	enable
Description	Activate the locator LED for this component
Configurable	True

duration *number*

Context	platform fan-tray id number locator enable duration number
Tree	duration
Description	Sets the duration to activate the locator LED, after which it will disable automatically
Range	10 to 3600
Units	seconds
Configurable	True

linecard **slot** *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number
Tree	linecard
Description	Operational commands related to line cards
Configurable	True

slot *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number
Description	Numeric identifier for the line card
Configurable	True

locator



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number locator
Tree	locator
Description	Operational commands for the locator LED
Configurable	True

disable



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number locator disable
Tree	disable
Description	Deactivates the locator LED for this component
Configurable	True

enable



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot number locator enable
Tree	enable
Description	Activate the locator LED for this component
Configurable	True

duration *number*



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> locator enable duration <i>number</i>
Tree	duration
Description	Sets the duration to activate the locator LED, after which it will disable automatically
Range	10 to 3600
Units	seconds
Configurable	True

reboot



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform linecard slot <i>number</i> reboot
Tree	reboot
Description	Reboot this component
Configurable	True

redundancy



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy
Tree	redundancy
Description	Top-level container for redundancy operational commands
Configurable	True

switchover



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy switchover
Tree	switchover
Description	Trigger a redundancy switchover to the other control module
Configurable	True

synchronize



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronize
Tree	synchronize
Description	Top-level container for manual synchronization activities
Configurable	True

overlay



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronize overlay
Tree	overlay
Description	Force a synchronization of the overlay filesystem between the active control module and the standby This synchronizes all non-excluded directories in the overlay filesystem
Configurable	True

system



Note: This command is available for the following platforms:

- 7250 IXR-6
- 7250 IXR-10

Context	platform redundancy synchronize system
Tree	system
Description	Force a synchronization of the system-required data between the active control module and the standby This synchronizes images, configuration, checkpoints, and other system-required data
Configurable	True

show-fabric-bandwidth

Context	platform show-fabric-bandwidth
Tree	show-fabric-bandwidth
Description	Show fabric bandwidth
Configurable	True

15 tools system

system

- + **app-management**
 - + **application name** *string*
 - + **kill**
 - + **quit**
 - + **reload**
 - + **restart**
 - + **start**
 - + **statistics**
 - + **clear**
 - + **stop**
- + **boot**
- + **configuration**
 - + **candidate name** *string*
 - + **clear**
 - + **checkpoint id** (*number | checkpoint-name*)
 - + **clear**
 - + **load**
 - + **revert**
 - + **confirmed-accept**
 - + **confirmed-reject**
 - + **generate-checkpoint**
 - + **comment** *string*
 - + **name** *string*
 - + **save**
 - + **session id** *number*
 - + **clear**
- + **packet-trace-base64**
 - + **interface** *string*
 - + **packet** *binary*
- + **traffic-monitor**
 - + **destination-address** *string*
 - + **source-address** *string*
 - + **destination-port** *value | value1..value2*
 - + **source-port** *value | value1..value2*
 - + **protocol** *value*
 - + **output-file** *filename*
 - + **hexdump**
 - + **verbose**
- + **tls**
 - + **generate-csr**
 - + **common-name** *string*
 - + **country** *string*
 - + **email** *string*
 - + **locality** *string*
 - + **organization** *string*
 - + **organization-unit** *string*
 - + **state** *string*
 - + **generate-self-signed**
 - + **common-name** *string*

- + **country** *string*
- + **duration** *number*
- + **email** *string*
- + **locality** *string*
- + **organization** *string*
- + **organization-unit** *string*
- + **state** *string*

15.1 system Descriptions

system

Context	system
Tree	system
Description	Enclosing container for system management.
Configurable	True

app-management

Context	system app-management
Tree	app-management
Description	Operational commands related to app-management
Configurable	True

application name *string*

Context	system app-management application name <i>string</i>
Tree	application
Description	List of all applications managed by the application manager
Configurable	True

name *string*

Context	system app-management application name <i>string</i>
Description	Unique name of this application instance
Configurable	True

kill

Context	system app-management application name <i>string</i> kill
Tree	kill
Description	Terminate the application instance ungracefully
Configurable	True

quit

Context	system app-management application name <i>string</i> quit
Tree	quit
Description	Terminate the application instance, requesting it to core dump
Configurable	True

reload

Context	system app-management application name <i>string</i> reload
Tree	reload
Description	Reload the configuration of the application instance
Configurable	True

restart

Context	system app-management application name <i>string</i> restart
Tree	restart
Description	Restart the application instance
Configurable	True

start

Context	system app-management application name <i>string</i> start
Tree	start
Description	Start the application instance
Configurable	True

statistics

Context	system app-management application name <i>string</i> statistics
Tree	statistics
Description	Top-level grouping of operational commands related to application statistics
Configurable	True

clear

Context	system app-management application name <i>string</i> statistics clear
Tree	clear
Description	Clear statistics for this application instance
Configurable	True

stop

Context	system app-management application name <i>string</i> stop
Tree	stop
Description	Terminate the application instance gracefully
Configurable	True

boot

Context	system boot
Tree	boot
Description	Top-level container for operational commands related to booting the system
Configurable	True

configuration

Context	system configuration
Tree	configuration
Description	Top-level container for operational commands related to the system configuration
Configurable	True

candidate name *string*

Context	system configuration candidate name <i>string</i>
Tree	candidate
Description	List of configuration candidates currently active
Configurable	True

name *string*

Context	system configuration candidate name <i>string</i>
Description	The name of the candidate
String Length	1 to 255
Configurable	True

clear

Context	system configuration candidate name <i>string</i> clear
Tree	clear
Description	Clear the candidate from the system, discarding any changes This results in any users currently in the candidate being dropped back to running mode.
Configurable	True

checkpoint id (*number | checkpoint-name*)

Context	system configuration checkpoint id (<i>number checkpoint-name</i>)
Tree	checkpoint
Description	List of current checkpoints present in the system
Configurable	True

id (*number | checkpoint-name*)

Context	system configuration checkpoint id (<i>number checkpoint-name</i>)
Description	System generated ID, or operator defined name for the checkpoint
Configurable	True

clear

Context	system configuration checkpoint id (<i>number checkpoint-name</i>) clear
Tree	clear
Description	Clear the checkpoint from the system
Configurable	True

load

Context	system configuration checkpoint id (<i>number checkpoint-name</i>) load
Tree	load
Description	Load candidate from saved checkpoint configuration
Configurable	True

revert

Context	system configuration checkpoint id (<i>number checkpoint-name</i>) revert
Tree	revert
Description	Revert running system configuration to the saved checkpoint configuration This functions as a load and commit action.
Configurable	True

confirmed-accept

Context	system configuration confirmed-accept
Tree	confirmed-accept
Description	Accepts an in progress commit and stops the confirmation timer
Configurable	True

confirmed-reject

Context	system configuration confirmed-reject
Tree	confirmed-reject
Description	Rejects an in progress commit and stops the confirmation timer
Configurable	True

generate-checkpoint

Context	system configuration generate-checkpoint
Tree	generate-checkpoint
Description	Generate a checkpoint point based on the current running configuration
Configurable	True

comment *string*

Context	system configuration generate-checkpoint comment <i>string</i>
Tree	comment
Description	User provided comment to associate with the checkpoint
Configurable	True

name *string*

Context	system configuration generate-checkpoint name <i>string</i>
Tree	name
Description	User provided name of the checkpoint
Configurable	True

save

Context	system configuration save
Tree	save
Description	Save current running configuration as initial config.json
Configurable	True

session id *number*

Context	system configuration session id <i>number</i>
Tree	session
Description	List of configuration sessions currently active
Configurable	True

id *number*

Context	system configuration session id <i>number</i>
Description	System generated ID for the configuration session
Configurable	True

clear

Context	system configuration session id <i>number</i> clear
Tree	clear
Description	Clear the session from the system, discarding any changes
Configurable	True

packet-trace-base64

Context	system packet-trace-base64
Tree	packet-trace-base64
Description	Tools command to report the forwarding behavior for a specified test packet (packet specified in base64 format)
Configurable	True

interface *string*

Context	system packet-trace-base64 interface <i>string</i>
Tree	interface
Description	References the configured name of the interface in which to inject the probe packet
Configurable	True

packet *binary*

Context	system packet-trace-base64 packet <i>binary</i>
Tree	packet
Description	Packet content encoded in base64 string format
Configurable	True

traffic-monitor

Context	system traffic-monitor
Tree	traffic-monitor
Description	Tools command to capture and report traffic ingressing the system with specific match criteria
Configurable	True
Presence	Configure tools system traffic-monitor

[destination-address] *string*

Context	system traffic-monitor destination-address
Tree	destination-address
Description	Specify destination IP address of traffic to match for the traffic-monitor tool
Configurable	True

[source-address] *string*

Context	system traffic-monitor source-address
Tree	source-address
Description	Specify source IP address of traffic to match for the traffic-monitor tool
Configurable	True

[destination-port] *value | value1..value2*

Context	system traffic-monitor destination-port
Tree	destination-port
Description	Specify destination port or range of traffic to match for the traffic-monitor tool (the protocol parameter must also be configured if this parameter is specified)
Configurable	True

[source-port] *value | value1..value2*

Context	system traffic-monitor source-port
Tree	source-port
Description	Specify source port or range of traffic to match for the traffic-monitor tool (the protocol parameter must also be configured if this parameter is specified)
Configurable	True

[protocol] *value*

Context	system traffic-monitor protocol
Tree	protocol
Description	Specify IP protocol type of traffic to match for the traffic-monitor tool
Configurable	True

[output-file] *filename*

Context	system traffic-monitor output-file
Tree	output-file
Description	Causes the redirection of output in pcap format to specified local file location (specified filename should include .pcap extension)
Configurable	True

[hexdump]

Context	system traffic-monitor hexdump
Tree	hexdump
Description	Causes the outputs packet data in to be expressed in hex and ASCII dump (Packet Bytes) format
Configurable	True

[verbose]

Context	system traffic-monitor verbose
Tree	verbose
Description	Causes the output to be displayed in a more verbose packet tree format (Packet Details)
Configurable	True

tls

Context	system tls
Tree	tls
Description	Top-level container for operational commands related to TLS
Configurable	True
Introduced	19.11.1

generate-csr

Context	system tls generate-csr
Tree	generate-csr
Description	Generates a certificate signing request and key pair

Fields for the certificate are taken from OpenSSL defaults, with the exception of the common name, which is taken from the system host name and domain name combination.

Configurable True
Introduced 20.4.1

common-name *string*

Context [system tls generate-csr common-name](#) *string*
Tree [common-name](#)
Description The common name to use for the certificate signing request
By default the common name is set to the system host name and domain name combination.
String Length 64
Configurable True
Introduced 20.4.1

country *string*

Context [system tls generate-csr country](#) *string*
Tree [country](#)
Description The country name to use for the certificate signing request
The expected format is two characters long, e.g. 'US'.
String Length 2
Default US
Configurable True
Introduced 20.4.1

email *string*

Context [system tls generate-csr email](#) *string*
Tree [email](#)
Description The email address to use for the certificate signing request
String Length 1 to 255
Configurable True
Introduced 20.4.1

locality *string*

Context	system tls generate-csr locality <i>string</i>
Tree	locality
Description	The city or locality to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	20.4.1

organization *string*

Context	system tls generate-csr organization <i>string</i>
Tree	organization
Description	The organization to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	20.4.1

organization-unit *string*

Context	system tls generate-csr organization-unit <i>string</i>
Tree	organization-unit
Description	The organization unit to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	20.4.1

state *string*

Context	system tls generate-csr state <i>string</i>
Tree	state
Description	The state or province to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	20.4.1

generate-self-signed

Context	system tls generate-self-signed
Tree	generate-self-signed
Description	Generates a self signed certificate and key pair Fields for the self signed certificate are taken from OpenSSL defaults, with the exception of the common name, which is taken from the system host name and domain name combination.
Configurable	True
Introduced	19.11.1

common-name *string*

Context	system tls generate-self-signed common-name <i>string</i>
Tree	common-name
Description	The common name to use for the certificate signing request By default the common name is set to the system host name and domain name combination.
String Length	64
Configurable	True
Introduced	19.11.1

country *string*

Context	system tls generate-self-signed country <i>string</i>
Tree	country
Description	The country name to use for the certificate signing request The expected format is two characters long, e.g. 'US'.
String Length	2
Default	US
Configurable	True
Introduced	19.11.1

duration *number*

Context	system tls generate-self-signed duration <i>number</i>
Tree	duration
Description	The time in which the certificate is valid
Range	1 to 3650
Default	365
Units	days
Configurable	True
Introduced	19.11.1

email *string*

Context	system tls generate-self-signed email <i>string</i>
Tree	email
Description	The email address to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	19.11.1

locality *string*

Context	system tls generate-self-signed locality <i>string</i>
Tree	locality
Description	The city or locality to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	19.11.1

organization *string*

Context	system tls generate-self-signed organization <i>string</i>
Tree	organization
Description	The organization to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	19.11.1

organization-unit *string*

Context	system tls generate-self-signed organization-unit <i>string</i>
Tree	organization-unit
Description	The organization unit to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	19.11.1

state *string*

Context	system tls generate-self-signed state <i>string</i>
Tree	state
Description	The state or province to use for the certificate signing request
String Length	1 to 255
Configurable	True
Introduced	19.11.1

Customer document and product support



Customer documentation

[Customer Documentation Welcome Page](#)



Technical Support

[Product Support Portal](#)



Documentation feedback

[Customer Documentation Feedback](#)

