



Nokia Service Router Linux

DATA MODEL REFERENCE RELEASE 22.3

**3HE 18313 AAAAA TQZZA
Issue 01**

March 2022

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com/terms/.

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks 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.

© 2022 Nokia.

Table of contents

1 About this guide.....	5
2 Overview.....	6
3 acl.....	10
4 bfd.....	623
5 interface.....	651
6 network-instance.....	858
7 platform.....	1531
8 qos.....	1662
9 routing-policy.....	1692
10 system.....	1715
11 tools acl.....	1974
12 tools bfd.....	1989
13 tools interface.....	1995
14 tools network-instance.....	2013
15 tools platform.....	2045
16 tools system.....	2056
17 tools tunnel.....	2081
18 tunnel-interface.....	2084

19 tunnel..... 2108

1 About this guide

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. See the *SR Linux Release Notes*, for information about features supported in each load.

For more information about accessing and using the interfaces that support these data models, see the *SR Linux System Management Guide*.

2 Overview

This overview describes the structure of the configuration and state data models available for the Nokia Service Router Linux (SR Linux). It includes an introduction to the tree hierarchy and details how to interpret field descriptions.

2.1 Tree hierarchy

The tree hierarchy consists of branches that show the fields and parameters that are available. [Figure 1: Tree hierarchy example](#) 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
  + peers number
  + clear
+ subinterface string
  + admin-state
  + desired-minimum-transmit-interval
  + detection-multiplier
  + minimum-echo-receive-interval
  + required-minimum-receive
+ total_bfd_sessions
+ total_unmatched_bfd_packets

```

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)*

2.2 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: Configuration/state in tree hierarchy](#).

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 System Management Guide*. These pre-defined reports can be used as examples for how to create additional custom reports.

2.3 Hardware platform designation

The platforms field is used to define the hardware platforms that are valid for a transaction. If a transaction is only valid on specific platforms, the designation is similar to the following:

*Figure 3: Platforms: applies to designated platforms only***name string**

Description	Enter the name context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source interface name <i>string</i>
String Length	3 to 20
Configurable	True
Platforms	7220 IXR-D3L, 7220 IXR-D3, 7220 IXR-D5, 7220 IXR-D2, 7220 IXR-D2L

If a transaction is valid on all platforms, the designation is the following:

*Figure 4: Platforms: applies to all platforms***acl**

Description	Top level enclosing container for ACL operational tools
Context	acl
Tree	acl
Configurable	True
Platforms	Supported on all platforms

2.4 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: Field descriptions](#) 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)

Field	Description
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
Platform	Defines the supported hardware platforms

2.4.1 References

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

3 acl

```

acl
+ capture-filter
+ ipv4-filter
  + entry sequence-id number
  + action
    + accept
    + copy
  + description string
  + match
    + destination-ip
      + address string
      + mask string
      + prefix string
    + destination-port
      + operator keyword
      + range
        + end (number | keyword)
        + start (number | keyword)
      + value (number | keyword)
    + dscp-set (number | keyword)
    + first-fragment boolean
    + fragment boolean
    + icmp
      + code number
      + type (number | keyword)
    + protocol (number | keyword)
    + source-ip
      + address string
      + mask string
      + prefix 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-ip
      + address string
      + mask string
      + prefix string
    + destination-port
      + operator keyword
      + range
        + end (number | keyword)
        + start (number | keyword)
      + value (number | keyword)
    + dscp-set (number | keyword)
    + icmp6
      + code number

```

```

+   + type (number | keyword)
+   + next-header (number | keyword)
+   + source-ip
+     + address string
+     + mask string
+     + prefix string
+   + source-port
+     + operator keyword
+     + range
+       + end (number | keyword)
+       + start (number | keyword)
+     + value (number | keyword)
+   + tcp-flags string
-   - 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-ip
+         + address string
+         + mask string
+         + prefix string
+       + destination-port
+         + operator keyword
+         + range
+           + end (number | keyword)
+           + start (number | keyword)
+         + value (number | keyword)
+     + dscp-set (number | keyword)
+     + first-fragment boolean
+     + fragment boolean
+     + icmp
+       + code number
+       + type (number | keyword)
+     + protocol (number | keyword)
+     + source-ip
+       + address string
+       + mask string
+       + prefix 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-ip
        + address string
        + mask string
        + prefix string
    + destination-port
        + operator keyword
        + range
            + end (number | keyword)
            + start (number | keyword)
        + value (number | keyword)
    + dscp-set (number | keyword)
    + icmp6
        + code number
        + type (number | keyword)
    + next-header (number | keyword)
    + source-ip
        + address string
        + mask string
        + prefix 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
+ mac-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-mac
    + address string
    + mask string
  + ethertype (string | keyword)
  + source-mac
    + address string
    + mask string
  + vlan
    + outermost-vlan-id
      + none
      + operator keyword
      + range
        + end number
        + start number
        + value number
  - 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
+ egress-mac-filtering boolean
+ ipv4-filter name string
+ description string
+ entry sequence-id number
+ action
  + accept
    + log boolean
  + drop
    + log boolean
+ description string
+ match
  + destination-ip
    + address string
    + mask string
    + prefix string
  + destination-port
    + operator keyword
    + range
      + end (number | keyword)
      + start (number | keyword)
      + value (number | keyword)
  + dscp-set (number | keyword)
  + first-fragment boolean
  + fragment boolean
  + icmp
    + code number
    + type (number | keyword)

```

```

+ protocol (number | keyword)
+ source-ip
+   address string
+   mask string
+   prefix 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-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-ip
+     address string
+     mask string
+     prefix string
+   destination-port
+     operator keyword
+     range
+       end (number | keyword)
+       start (number | keyword)
+     value (number | keyword)
+   dscp-set (number | keyword)
+   icmp6
+     code number
+     type (number | keyword)
+   next-header (number | keyword)
+   source-ip
+     address string
+     mask string
+     prefix 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-per-entry boolean
+ subinterface-specific keyword
+ mac-filter name string
+ description string
+ entry sequence-id number
+ action
  + accept
    + log boolean
  + drop
    + log boolean
+ description string
+ match
  + destination-mac
    + address string
    + mask string
  + ethertype (string | keyword)
  + source-mac
    + address string
    + mask string
  + vlan
    + outermost-vlan-id
      + none
      + operator keyword
      + range
        + end number
        + start number
        + value number
- 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-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
+ system-filter
+ ipv4-filter
+ entry sequence-id number
+ action
+ accept
+ drop
+ log boolean
+ description string
+ match
+ destination-ip
+ address string
+ mask string
+ prefix string
+ destination-port
+ operator keyword
+ range
+ end (number | keyword)
+ start (number | keyword)
+ value (number | keyword)
+ dscp-set (number | keyword)
+ first-fragment boolean
+ fragment boolean
+ icmp
+ code number
+ type (number | keyword)
+ protocol (number | keyword)
+ source-ip
+ address string
+ mask string
+ prefix string
+ source-port
+ operator keyword
+ range
+ end (number | keyword)
+ start (number | keyword)
+ value (number | keyword)
+ tcp-flags string
- statistics

```

```

    - last-clear string
    - last-match string
    - matched-packets number
    - tcam-entries number
- last-clear string
+ ipv6-filter
+ entry sequence-id number
+ action
+ accept
+ drop
+ log boolean
+ description string
+ match
+ destination-ip
+ address string
+ mask string
+ prefix string
+ destination-port
+ operator keyword
+ range
+ end (number | keyword)
+ start (number | keyword)
+ value (number | keyword)
+ dscp-set (number | keyword)
+ icmp6
+ code number
+ type (number | keyword)
+ next-header (number | keyword)
+ source-ip
+ address string
+ mask string
+ prefix string
+ source-port
+ operator keyword
+ range
+ end (number | keyword)
+ start (number | keyword)
+ value (number | keyword)
+ tcp-flags string
- statistics
- last-clear string
- last-match string
- matched-packets number
- tcam-entries number
- last-clear string
+ tcam-profile keyword

```

3.1 acl Descriptions

acl

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

capture-filter

Description	Top level container for capture filters
Context	acl capture-filter
Tree	capture-filter
Configurable	True
Platforms	Supported on all platforms

ipv4-filter

Description	Top level container for capture IPv4 filters
Context	acl capture-filter ipv4-filter
Tree	ipv4-filter
Configurable	True
Platforms	Supported on all platforms

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

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

sequence-id *number*

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

action

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

accept

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

copy

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

description *string*

Description	Description string for the filter entry
--------------------	---

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

match

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

destination-ip

Description	Packet matching criteria based on destination IPv4 address
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-ip
Tree	destination-ip
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-ip address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask *string*

Description	Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.
--------------------	--

Context	acl capture-filter ipv4-filter entry sequence-id number match destination-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its destination IP address is within the specified IPv4 prefix.
Context	acl capture-filter ipv4-filter entry sequence-id number match destination-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl capture-filter ipv4-filter entry sequence-id number match destination-port
Tree	destination-port
Configurable	True
Platforms	Supported on all platforms

operator keyword

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

Equal to.

Configurable	True
Platforms	Supported on all platforms

range

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

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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

-
- 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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms Supported on all platforms

value (*number* | *keyword*)

Description	A destination port number
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match destination-port <i>value</i> (<i>number</i> <i>keyword</i>)
Tree	value
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
Platforms	Supported on all platforms

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
Range	0 to 63
Options	<ul style="list-style-type: none"> • CS0 • LE • CS1 • AF11 • AF12 • AF13 • CS2 • AF21 • AF22 • AF23 • CS3 • AF31

	<ul style="list-style-type: none"> • AF32 • AF33 • CS4 • AF41 • AF42 • AF43 • CS5 • EF • CS6 • CS7
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

first-fragment *boolean*

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.
Context	acl capture-filter ipv4-filter entry sequence-id number match first-fragment boolean
Tree	first-fragment
Configurable	True
Platforms	Supported on all platforms

fragment *boolean*

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.
Context	acl capture-filter ipv4-filter entry sequence-id number match fragment boolean
Tree	fragment
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl capture-filter ipv4-filter entry sequence-id number match icmp
Tree	icmp
Configurable	True
Platforms	Supported on all platforms

code number

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

type (number | keyword)

Description	Match a single ICMP type value.
Context	acl capture-filter ipv4-filter entry sequence-id number match icmp type (number keyword)
Tree	type
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
Platforms	Supported on all platforms

protocol (*number* | *keyword*)

Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match protocol (<i>number</i> <i>keyword</i>)
Tree	protocol
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
 - `ospf`
OSPFv2 and OSPFv3
 - `pim`
Protocol Independent Multicast
 - `vrrp`
Virtual Router Redundancy Protocol
 - `l2tp`
Layer Two Tunneling Protocol
 - `sctp`
Stream Control Transmission Protocol

	<ul style="list-style-type: none"> mpls-in-ip MPLS Encapsulation inside IP rohc Robust Header Compression
Configurable	True
Platforms	Supported on all platforms

source-ip

Description	Packet matching criteria based on source IPv4 address
Context	acl capture-filter ipv4-filter entry sequence-id number match source-ip
Tree	source-ip
Configurable	True
Platforms	Supported on all platforms

address string

Description	Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context	acl capture-filter ipv4-filter entry sequence-id number match source-ip address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask string

Description	Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl capture-filter ipv4-filter entry sequence-id number match source-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its source IP address is within the specified IPv4 prefix.
--------------------	--

Context	acl capture-filter ipv4-filter entry sequence-id number match source-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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>
Context	acl capture-filter ipv4-filter entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

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

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
--------------------	--

Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port range
Tree	range
Configurable	True
Platforms	Supported on all platforms

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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

-
- 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)
 - ldap
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl capture-filter ipv4-filter entry sequence-id number match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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)
 - sgmpp
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)
- `xmcp`
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
Platforms	Supported on all platforms

value (*number* | *keyword*)

Description	A source port number
Context	acl capture-filter ipv4-filter entry sequence-id <i>number</i> match source-port value (<i>number</i> <i>keyword</i>)

Tree	value
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)
 - sgmpp
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

tcp-flags *string*

Description	A logical expression using the &, and ! logical operators and the TCP flag names: rst, syn and ack.
Context	acl capture-filter ipv4-filter entry sequence-id number match tcp-flags string
Tree	tcp-flags
Configurable	True
Platforms	Supported on all platforms

tcam-entries *number*

Description	The number of TCAM entries required to implement a single instance of this filter rule.
Context	acl capture-filter ipv4-filter entry sequence-id number tcam-entries number
Tree	tcam-entries
Configurable	False
Platforms	Supported on all platforms

ipv6-filter

Description	Top level container for capture IPv6 filters
Context	acl capture-filter ipv6-filter
Tree	ipv6-filter
Configurable	True
Platforms	Supported on all platforms

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

Description	List of filter rules.
--------------------	-----------------------

Context	acl capture-filter ipv6-filter entry sequence-id number
Tree	entry
Configurable	True
Platforms	Supported on all platforms

sequence-id *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl capture-filter ipv6-filter entry sequence-id number
Range	1 to 65535
Configurable	True
Platforms	Supported on all platforms

action

Description	Container for the actions to be applied to packets matching the capture filter entry.
Context	acl capture-filter ipv6-filter entry sequence-id number action
Tree	action
Configurable	True
Platforms	Supported on all platforms

accept

Description	Accept matching packets and forward them towards their normal destination
Context	acl capture-filter ipv6-filter entry sequence-id number action accept
Tree	accept
Configurable	True
Platforms	Supported on all platforms

copy

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

Configurable	True
Platforms	Supported on all platforms

description *string*

Description	Description string for the filter entry
Context	acl capture-filter ipv6-filter entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	acl capture-filter ipv6-filter entry sequence-id number match
Tree	match
Configurable	True
Platforms	Supported on all platforms

destination-ip

Description	Packet matching criteria based on destination IPv6 address
Context	acl capture-filter ipv6-filter entry sequence-id number match destination-ip
Tree	destination-ip
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl capture-filter ipv6-filter entry sequence-id number match destination-ip address string
Tree	address
Configurable	True

Platforms Supported on all platforms

mask *string*

Description Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.

Context [acl capture-filter ipv6-filter entry sequence-id number match destination-ip mask string](#)

Tree [mask](#)

Configurable True

Platforms Supported on all platforms

prefix *string*

Description Match a packet if its destination IP address is within the specified IPv6 prefix.

Context [acl capture-filter ipv6-filter entry sequence-id number match destination-ip prefix string](#)

Tree [prefix](#)

Configurable True

Platforms Supported on all platforms

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.

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

Tree [destination-port](#)

Configurable True

Platforms Supported on all platforms

operator *keyword*

Description Comparison operator
eq = equal ge = greater than or equal to le = less than or equal to

Context [acl capture-filter ipv6-filter entry sequence-id number match destination-port operator keyword](#)

Tree	operator
Options	<ul style="list-style-type: none"> • <code>le</code> Less than or equal. • <code>ge</code> Greater than or equal. • <code>eq</code> Equal to.
Configurable	True
Platforms	Supported on all platforms

range

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

end (*number* | *keyword*)

Description	The ending port number to include in the range
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
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

- 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)
- `xmcp`
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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range start (<i>number</i> <i>keyword</i>)

Tree	start
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)
 - sgmpp
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

value (*number* | *keyword*)

Description	A destination port number
Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match destination-port <i>value</i> (<i>number</i> <i>keyword</i>)
Tree	value
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
Platforms	Supported on all platforms

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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

Platforms

7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.

Context

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

Tree

[icmp6](#)

Configurable

True

Platforms

Supported on all platforms

code number**Description**

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

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

Context

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

Tree

[code](#)

Configurable	True
Platforms	Supported on all platforms

type (*number* | *keyword*)

Description	Match a single ICMPv6 type value
Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match icmp6 type (<i>number</i> <i>keyword</i>)
Tree	type
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 • <code>neighbor-advertise</code> ICMPv6 Neighbor Advertisement • <code>redirect</code>

	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
Platforms	Supported on all platforms

next-header (*number* | *keyword*)

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

-
- 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
 - ospf
OSPFv2 and OSPFv3
 - 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
Platforms Supported on all platforms

source-ip

Description Packet matching criteria based on source IPv6 address
Context [acl capture-filter ipv6-filter entry sequence-id number match source-ip](#)
Tree [source-ip](#)
Configurable True
Platforms Supported on all platforms

address string

Description Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context [acl capture-filter ipv6-filter entry sequence-id number match source-ip address string](#)
Tree [address](#)
Configurable True
Platforms Supported on all platforms

mask string

Description Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context [acl capture-filter ipv6-filter entry sequence-id number match source-ip mask string](#)
Tree [mask](#)
Configurable True
Platforms Supported on all platforms

prefix string

Description	Match a packet if its source IP address is within the specified IPv6 prefix.
Context	acl capture-filter ipv6-filter entry sequence-id number match source-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl capture-filter ipv6-filter entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	Supported on all platforms

operator keyword

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

range

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

end (*number* | *keyword*)

Description	The ending port number to include in the range
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
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
 - 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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
Platforms**

True
Supported on all platforms

value (*number* | *keyword*)

Description	A source port number
Context	acl capture-filter ipv6-filter entry sequence-id <i>number</i> match source-port <i>value</i> (<i>number</i> <i>keyword</i>)
Tree	value
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
 - BFDD 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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

tcp-flags *string*

Description	A logical expression using the &, and ! logical operators and the TCP flag names: rst, syn and ack.
Context	acl capture-filter ipv6-filter entry sequence-id number match tcp-flags string
Tree	tcp-flags
Configurable	True
Platforms	Supported on all platforms

tcam-entries *number*

Description	The number of TCAM entries required to implement a single instance of this filter rule.
Context	acl capture-filter ipv6-filter entry sequence-id number tcam-entries number
Tree	tcam-entries
Configurable	False
Platforms	Supported on all platforms

cpm-filter

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

Configurable	True
Platforms	Supported on all platforms

ipv4-filter

Description	Top level container for CPM IPv4 filters
Context	acl cpm-filter ipv4-filter
Tree	ipv4-filter
Configurable	True
Platforms	Supported on all platforms

entry [sequence-id number](#)

Description	List of filter rules.
Context	acl cpm-filter ipv4-filter entry sequence-id number
Tree	entry
Configurable	True
Platforms	Supported on all platforms

sequence-id *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl cpm-filter ipv4-filter entry sequence-id number
Range	1 to 65535
Configurable	True
Platforms	Supported on all platforms

action

Description	Container for the actions to be applied to packets matching the CPM filter entry.
Context	acl cpm-filter ipv4-filter entry sequence-id number action
Tree	action
Configurable	True
Platforms	Supported on all platforms

accept

Description	Accept matching packets and forward them towards their normal destination
Context	acl cpm-filter ipv4-filter entry sequence-id number action accept
Tree	accept
Configurable	True
Platforms	Supported on all platforms

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl cpm-filter ipv4-filter entry sequence-id number action accept log boolean
Tree	log
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

rate-limit

Description	Rate-limit accepted packets
Context	acl cpm-filter ipv4-filter entry sequence-id number action accept rate-limit
Tree	rate-limit
Configurable	True
Platforms	Supported on all platforms

distributed-policer *reference*

Description	Reference to a policer
Context	acl cpm-filter ipv4-filter entry sequence-id number action accept rate-limit distributed-policer reference
Tree	distributed-policer
Reference	acl policers policer name string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

system-cpu-policer *reference*

Description	Reference to a system-cpu-policer.
Context	acl cpm-filter ipv4-filter entry sequence-id number action accept rate-limit system-cpu-policer reference
Tree	system-cpu-policer
Reference	acl policers system-cpu-policer name string
Configurable	True
Platforms	Supported on all platforms

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl cpm-filter ipv4-filter entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	Supported on all platforms

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl cpm-filter ipv4-filter entry sequence-id number action drop log boolean
Tree	log
Default	false
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	Description string for the filter entry
Context	acl cpm-filter ipv4-filter entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	acl cpm-filter ipv4-filter entry sequence-id number match
Tree	match
Configurable	True
Platforms	Supported on all platforms

destination-ip

Description	Packet matching criteria based on destination IPv4 address
Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-ip
Tree	destination-ip
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-ip address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask *string*

Description	Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its destination IP address is within the specified IPv4 prefix.
Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl cpm-filter ipv4-filter entry sequence-id number match destination-port
Tree	destination-port
Configurable	True
Platforms	Supported on all platforms

operator keyword

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

range

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

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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
 - 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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match destination-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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

Platforms

Supported on all platforms

value (*number* | *keyword*)

Description	A destination port number
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match destination-port value (<i>number</i> <i>keyword</i>)
Tree	value
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
 - BFDD 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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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

	<ul style="list-style-type: none"> • CS4 • AF41 • AF42 • AF43 • CS5 • EF • CS6 • CS7
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

first-fragment *boolean*

Description	<p>Match the first fragment of an IPv4 datagram</p> <p>A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero and the more-fragments bit is 1. It is not valid to configure this leaf without configuring a match value for the fragment leaf.</p>
Context	acl cpm-filter ipv4-filter entry sequence-id number match first-fragment boolean
Tree	first-fragment
Configurable	True
Platforms	Supported on all platforms

fragment *boolean*

Description	<p>Match an IPv4 fragment</p> <p>A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero 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.</p>
Context	acl cpm-filter ipv4-filter entry sequence-id number match fragment boolean
Tree	fragment
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl cpm-filter ipv4-filter entry sequence-id number match icmp
Tree	icmp
Configurable	True
Platforms	Supported on all platforms

code number

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

type (number | keyword)

Description	Match a single ICMP type value.
Context	acl cpm-filter ipv4-filter entry sequence-id number match icmp type (number keyword)
Tree	type
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
Platforms	Supported on all platforms

protocol (*number* | *keyword*)

Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match protocol (<i>number</i> <i>keyword</i>)
Tree	protocol
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
 - ospf
OSPFv2 and OSPFv3
 - 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
Platforms	Supported on all platforms

source-ip

Description	Packet matching criteria based on source IPv4 address
Context	acl cpm-filter ipv4-filter entry sequence-id number match source-ip
Tree	source-ip
Configurable	True
Platforms	Supported on all platforms

address string

Description	Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context	acl cpm-filter ipv4-filter entry sequence-id number match source-ip address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask string

Description	Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl cpm-filter ipv4-filter entry sequence-id number match source-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its source IP address is within the specified IPv4 prefix.
Context	acl cpm-filter ipv4-filter entry sequence-id number match source-ip prefix string

Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl cpm-filter ipv4-filter entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

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

range

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

Platforms Supported on all platforms

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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)
 - sgmplib
 - 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
	<ul style="list-style-type: none"> • 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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
Platforms	Supported on all platforms

value (*number | keyword*)

Description	A source port number
Context	acl cpm-filter ipv4-filter entry sequence-id number match source-port value (<i>number keyword</i>)
Tree	value
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)

- Idaps
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
- Idp
Label Distribution Protocol
- Imp
Link Management Protocol (LMP)
- login
rlogin (TCP) or Who (UDP)
- Ipd
Line Printer Daemon
- Isp-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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

tcp-flags *string*

Description	A logical expression using the &, and ! logical operators and the TCP flag names: rst, syn and ack.
Context	acl cpm-filter ipv4-filter entry sequence-id number match tcp-flags string
Tree	tcp-flags
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Statistics container for packets matching the CPM-filter entry
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

distributed-policer

Description	Distributed policer stats for traffic matching the entry.
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer
Tree	distributed-policer
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-octets *number*

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.
--------------------	--

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer conforming-octets number
Tree	conforming-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer conforming-packets number
Tree	conforming-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-octets *number*

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.
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics distributed-policer exceeding-octets number
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-packets *number*

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

Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-match *string*

Description	The elapsed time since a packet last matched the entry, considering all subinterfaces and all linecards.
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics last-match string
Tree	last-match
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

matched-packets *number*

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

system-cpu-policer

Description	System CPU policer stats for traffic matching the entry.
--------------------	--

Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer
Tree	system-cpu-policer
Configurable	False
Platforms	Supported on all platforms

conforming-octets *number*

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.
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer conforming-octets number
Tree	conforming-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

conforming-packets *number*

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

exceeding-octets *number*

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.
Context	acl cpm-filter ipv4-filter entry sequence-id number statistics system-cpu-policer exceeding-octets number
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

exceeding-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics system-cpu-policer exceeding-packets <i>number</i>
Tree	exceeding-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

tcam-entries *number*

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

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl cpm-filter ipv4-filter last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

statistics-per-entry *boolean*

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
Context	acl cpm-filter ipv4-filter statistics-per-entry <i>boolean</i>
Tree	statistics-per-entry
Configurable	True
Platforms	Supported on all platforms

ipv6-filter

Description	Top level container for CPM IPv6 filters
Context	acl cpm-filter ipv6-filter
Tree	ipv6-filter
Configurable	True
Platforms	Supported on all platforms

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

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

[sequence-id](#) *number*

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

action

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

accept

Description	Accept matching packets and forward them towards their normal destination
--------------------	---

Context	acl cpm-filter ipv6-filter entry sequence-id number action accept
Tree	accept
Configurable	True
Platforms	Supported on all platforms

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl cpm-filter ipv6-filter entry sequence-id number action accept log boolean
Tree	log
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

rate-limit

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

distributed-policer *reference*

Description	Reference to a policer
Context	acl cpm-filter ipv6-filter entry sequence-id number action accept rate-limit distributed-policer reference
Tree	distributed-policer
Reference	acl policers policer name string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

system-cpu-policer *reference*

Description	Reference to a system-cpu-policer.
--------------------	------------------------------------

Context	acl cpm-filter ipv6-filter entry sequence-id number action accept rate-limit system-cpu-policer <i>reference</i>
Tree	system-cpu-policer
Reference	acl policers system-cpu-policer name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl cpm-filter ipv6-filter entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	Supported on all platforms

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl cpm-filter ipv6-filter entry sequence-id number action drop log <i>boolean</i>
Tree	log
Default	false
Configurable	True
Platforms	Supported on all platforms

description *string*

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

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	acl cpm-filter ipv6-filter entry sequence-id number match
Tree	match
Configurable	True
Platforms	Supported on all platforms

destination-ip

Description	Packet matching criteria based on destination IPv6 address
Context	acl cpm-filter ipv6-filter entry sequence-id number match destination-ip
Tree	destination-ip
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl cpm-filter ipv6-filter entry sequence-id number match destination-ip address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask *string*

Description	Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl cpm-filter ipv6-filter entry sequence-id number match destination-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its destination IP address is within the specified IPv6 prefix.
Context	acl cpm-filter ipv6-filter entry sequence-id number match destination-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl cpm-filter ipv6-filter entry sequence-id number match destination-port destination-port
Tree	destination-port
Configurable	True
Platforms	Supported on all platforms

operator keyword

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

range

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

end (*number* | *keyword*)

Description	The ending port number to include in the range
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
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
 - 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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
Platforms**

True
Supported on all platforms

value (*number* | *keyword*)

Description	A destination port number
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match destination-port value (<i>number</i> <i>keyword</i>)
Tree	value
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)
- tcpnethaspsrv
tcpnethaspsrv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups

	Uninterruptible power supply (UPS)
	<ul style="list-style-type: none"> • 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
Platforms	Supported on all platforms

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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

	<ul style="list-style-type: none"> • CS4 • AF41 • AF42 • AF43 • CS5 • EF • CS6 • CS7
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

icmp6

Description	<p>A packet matches this condition if its ICMPv6 type and code matches one of the specified combinations</p> <p>The rule should also have a condition that the next-header value equals 58 (ICMPv6) in order for this to be interpreted correctly.</p>
Context	acl cpm-filter ipv6-filter entry sequence-id number match icmp6
Tree	icmp6
Configurable	True
Platforms	Supported on all platforms

code number

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

type (number | keyword)

Description	Match a single ICMPv6 type value
Context	acl cpm-filter ipv6-filter entry sequence-id number match icmp6 type (number keyword)

Tree	type
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
Platforms	Supported on all platforms

next-header (*number* | *keyword*)

Description	An IPv6 packet matches this condition if its first next-header field (in the IPv6 fixed header) contains the specified value
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match next-header (<i>number</i> <i>keyword</i>)
Tree	next-header
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
- ospf
 - OSPFv2 and OSPFv3
- 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
Platforms**

True
Supported on all platforms

source-ip

Description	Packet matching criteria based on source IPv6 address
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-ip
Tree	source-ip
Configurable	True
Platforms	Supported on all platforms

address string

Description	Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-ip address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask string

Description	Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-ip mask <i>string</i>
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its source IP address is within the specified IPv6 prefix.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-ip prefix <i>string</i>
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl cpm-filter ipv6-filter entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

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

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl cpm-filter ipv6-filter entry sequence-id number match source-port range
Tree	range
Configurable	True
Platforms	Supported on all platforms

end (*number* | *keyword*)

Description	The ending port number to include in the range
--------------------	--

Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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)
- tcpnethaspsrv
tcpnethaspsrv, 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)
	<ul style="list-style-type: none"> xns-mail
	Xerox Network Systems (XNS) Mail
	<ul style="list-style-type: none"> xns-time
	Xerox Network Systems (XNS) Time Protocol
	<ul style="list-style-type: none"> z3950
	ANSI Z39.50
Configurable	True
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
Platforms	Supported on all platforms

value (*number* | *keyword*)

Description	A source port number
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match source-port value (<i>number</i> <i>keyword</i>)
Tree	value
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

Platforms

Supported on all platforms

tcp-flags *string*

Description	A logical expression using the &, and ! logical operators and the TCP flag names: rst, syn and ack.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> match tcp-flags <i>string</i>
Tree	tcp-flags
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Statistics container for packets matching the CPM-filter entry
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

distributed-policer

Description	Distributed policer stats for traffic matching the entry.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics distributed-policer
Tree	distributed-policer
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-octets *number*

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.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics distributed-policer conforming-octets <i>number</i>
Tree	conforming-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics distributed-policer conforming-packets <i>number</i>
Tree	conforming-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-octets *number*

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.
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics distributed-policer exceeding-octets <i>number</i>
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Context	acl cpm-filter ipv6-filter entry sequence-id <i>number</i> statistics distributed-policer exceeding-packets <i>number</i>
Tree	exceeding-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

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

Context	acl cpm-filter ipv6-filter entry sequence-id number statistics last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-match string

Description	The elapsed time since a packet last matched the entry, considering all subinterfaces and all linecards.
Context	acl cpm-filter ipv6-filter entry sequence-id number statistics last-match string
Tree	last-match
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

matched-packets number

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

system-cpu-policer

Description	System CPU policer stats for traffic matching the entry.
Context	acl cpm-filter ipv6-filter entry sequence-id number statistics system-cpu-policer
Tree	system-cpu-policer
Configurable	False
Platforms	Supported on all platforms

conforming-octets *number*

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.
Context	acl cpm-filter ipv6-filter entry sequence-id number statistics system-cpu-policer conforming-octets number
Tree	conforming-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

conforming-packets *number*

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

exceeding-octets *number*

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.
Context	acl cpm-filter ipv6-filter entry sequence-id number statistics system-cpu-policer exceeding-octets number
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

exceeding-packets *number*

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

Default	0
Configurable	False
Platforms	Supported on all platforms

tcam-entries *number*

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

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl cpm-filter ipv6-filter last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

statistics-per-entry *boolean*

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
Context	acl cpm-filter ipv6-filter statistics-per-entry <i>boolean</i>
Tree	statistics-per-entry
Configurable	True
Platforms	Supported on all platforms

mac-filter

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

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

entry *sequence-id number*

Description List of filter rules.

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

Tree [entry](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

sequence-id *number*

Description A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries

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

Range 1 to 65535

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action

Description Container for the actions to be applied to packets matching the CPM filter entry.

Context [acl cpm-filter mac-filter entry sequence-id number action](#)

Tree [action](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

accept

Description Accept matching packets and forward them towards their normal destination

Context [acl cpm-filter mac-filter entry sequence-id number action accept](#)

Tree [accept](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl cpm-filter mac-filter entry sequence-id number action accept log boolean
Tree	log
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

rate-limit

Description	Rate-limit accepted packets
Context	acl cpm-filter mac-filter entry sequence-id number action accept rate-limit
Tree	rate-limit
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

distributed-policer *reference*

Description	Reference to a policer
Context	acl cpm-filter mac-filter entry sequence-id number action accept rate-limit distributed-policer reference
Tree	distributed-policer
Reference	acl policers policer name string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

system-cpu-policer *reference*

Description	Reference to a system-cpu-policer.
Context	acl cpm-filter mac-filter entry sequence-id number action accept rate-limit system-cpu-policer reference
Tree	system-cpu-policer
Reference	acl policers system-cpu-policer name string
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> action drop
Tree	drop
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> action drop log <i>boolean</i>
Tree	log
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description *string*

Description	Description string for the filter entry
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

match

Description	Container for the conditions that determine whether an Ethernet frame matches this entry
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> match
Tree	match
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-mac

Description	Ethernet frame matching criteria based on destination MAC address
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> match destination-mac
Tree	destination-mac
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Match an Ethernet frame if its destination MAC address logically anded with the mask equals this MAC address.
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> match destination-mac address <i>string</i>
Tree	address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask string

Description	Match an Ethernet frame if its destination MAC address logically anded with the mask equals the configured MAC address.
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> match destination-mac mask <i>string</i>
Tree	mask
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ethertype (string | keyword)

Description	An Ethernet frame matches this condition if its ethertype value (after 802.1Q VLAN tags) matches the specified value
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> match ethertype (<i>string</i> <i>keyword</i>)
Tree	ethertype
Options	<ul style="list-style-type: none"> • <code>ipv4</code> Internet Protocol version 4. Ethertype 0x0800. • <code>arp</code>

- Address Resolution Protocol. Ethertype 0x0806.
- ipv6
Internet Protocol version 6. Ethertype 0x86DD.
- flow-control
Ethernet flow control PAUSE frames. Ethertype 0x8808
- lacp
LACP. Ethertype 0x8809.
- mpls-unicast
MPLS unicast. Ethertype 0x8847.
- mpls-multicast
MPLS multicast. Ethertype 0x8848.
- pppoe-discovery
PPPoE discovery. Ethertype 0x8863.
- pppoe-session
PPPoE session. Ethertype 0x8864.
- 8021x-authentication
802.1x authentication (EAP). Ethertype 0x888E.
- lldp
Link Layer Discovery Protocol. Ethertype 0x88CC.
- macsec
IEEE 802.1AE MAC security. Ethertype 0x88E5.
- pbb
Provider Backbone Bridging. Ethertype 0x88E7.
- ptp
Precision Time Protocol. Ethertype 0x88F7.
- eth-oam
IEEE 802.1ag CFM and ITU-T Y.1731 OAM. Ethertype 0x8902.
- fcoe
Fibre Channel over Ethernet. Ethertype 0x8906.
- fcoe-initialization
Fibre Channel over Ethernet Initialization Protocol. Ethertype 0x8914.
- roce
RDMA over Converged Ethernet. Ethertype 0x8915.

**Configurable
Platforms**

True

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

source-mac

Description	Ethernet frame matching criteria based on source MAC address
Context	acl cpm-filter mac-filter entry sequence-id number match source-mac
Tree	source-mac
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Match an Ethernet frame if its source MAC address logically anded with the mask equals this MAC address.
Context	acl cpm-filter mac-filter entry sequence-id number match source-mac address string
Tree	address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask string

Description	Match an Ethernet frame if its source MAC address logically anded with the mask equals the configured MAC address.
Context	acl cpm-filter mac-filter entry sequence-id number match source-mac mask string
Tree	mask
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

vlan

Description	Ethernet frame matching criteria based on VLAN tags
Context	acl cpm-filter mac-filter entry sequence-id number match vlan
Tree	vlan
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

outermost-vlan-id

Description	Ethernet frame matching criteria based on the outermost VLAN ID found before the subinterface-defining VLAN tag (if any) is removed.
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id
Tree	outermost-vlan-id
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

none

Description	When configured, only untagged frames are matched.
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id none
Tree	none
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

operator *keyword*

Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id operator keyword
Tree	operator
Options	<ul style="list-style-type: none"> • le Less than or equal. • ge Greater than or equal. • eq Equal to.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

range

Description	Container used to specify a contiguous range of VLAN IDs. Matched values include the start and end values.
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id range
Tree	range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

end number

Description	The ending VLAN ID to include in the range
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id range end number
Tree	end
Range	0 to 4095
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

start number

Description	The starting VLAN ID to include in the range
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id range start number
Tree	start
Range	0 to 4095
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

value number

Description	A VLAN ID number A value of zero is used to match priority-tagged 802.1Q frames.
Context	acl cpm-filter mac-filter entry sequence-id number match vlan outermost-vlan-id value number
Tree	value
Range	0 to 4095

Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description	Statistics container for packets matching the CPM-filter entry
Context	acl cpm-filter mac-filter entry sequence-id number statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

distributed-policer

Description	Distributed policer stats for traffic matching the entry.
Context	acl cpm-filter mac-filter entry sequence-id number statistics distributed-policer
Tree	distributed-policer
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-octets *number*

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.
Context	acl cpm-filter mac-filter entry sequence-id number statistics distributed-policer conforming-octets number
Tree	conforming-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Context	acl cpm-filter mac-filter entry sequence-id number statistics distributed-policer conforming-packets number

Tree	conforming-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-octets *number*

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.
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics distributed-policer exceeding-octets <i>number</i>
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics distributed-policer exceeding-packets <i>number</i>
Tree	exceeding-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-match string

Description	The elapsed time since a packet last matched the entry, considering all subinterfaces and all linecards.
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics last-match <i>string</i>
Tree	last-match
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

matched-packets number

Description	The number of packets matching the entry since it was programmed or since the last clear, summed across all subinterfaces and all linecards
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics matched-packets <i>number</i>
Tree	matched-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

system-cpu-policer

Description	System CPU policer stats for traffic matching the entry.
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics system-cpu-policer
Tree	system-cpu-policer
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-octets number

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.
Context	acl cpm-filter mac-filter entry sequence-id <i>number</i> statistics system-cpu-policer conforming-octets <i>number</i>
Tree	conforming-octets
Default	0

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered conforming by the policer
Context	acl cpm-filter mac-filter entry sequence-id number statistics system-cpu-policer conforming-packets number
Tree	conforming-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-octets *number*

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.
Context	acl cpm-filter mac-filter entry sequence-id number statistics system-cpu-policer exceeding-octets number
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-packets *number*

Description	The number of packets (actually Ethernet frames) that were considered exceeding by the policer
Context	acl cpm-filter mac-filter entry sequence-id number statistics system-cpu-policer exceeding-packets number
Tree	exceeding-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcam-entries *number*

Description	The number of TCAM entries required to implement a single instance of this filter rule.
Context	acl cpm-filter mac-filter entry sequence-id number tcam-entries number
Tree	tcam-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl cpm-filter mac-filter last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics-per-entry *boolean*

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
Context	acl cpm-filter mac-filter statistics-per-entry boolean
Tree	statistics-per-entry
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

egress-mac-filtering *boolean*

Description	<p>Must be set to true in order to apply any MAC ACLs to any subinterface in the egress traffic direction.</p> <p>Internally this sets the following limits:</p> <p>Remember that the number of ACL instances per ACL policy is greater than one if subinterface-specific is set to input-and-output or output-only.</p> <p>A setting of true is blocked if the number of IPv4 ACL instances applied to egress traffic is already greater than 32, or if the number of IPv6 ACL instances applied to egress traffic is already greater than 32.</p>
Context	acl egress-mac-filtering boolean
Tree	egress-mac-filtering

Default	false
Configurable	True
Platforms	Supported on all platforms

ipv4-filter *name string*

Description	List of IPv4 filter policies
Context	acl ipv4-filter name string
Tree	ipv4-filter
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of the IPv4 filter policy.
Context	acl ipv4-filter name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	Description string for the IPv4 filter policy
Context	acl ipv4-filter name string description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

entry *sequence-id number*

Description	List of filter rules.
Context	acl ipv4-filter name string entry sequence-id number
Tree	entry
Configurable	True
Platforms	Supported on all platforms

sequence-id *number*

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

action

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

accept

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

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl ipv4-filter name <i>string</i> entry sequence-id number action accept log <i>boolean</i>
Tree	log
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl ipv4-filter name string entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	Supported on all platforms

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: 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.
Context	acl ipv4-filter name string entry sequence-id number action drop log boolean
Tree	log
Default	false
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	Description string for the filter entry
Context	acl ipv4-filter name string entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	acl ipv4-filter name string entry sequence-id number match
Tree	match
Configurable	True
Platforms	Supported on all platforms

destination-ip

Description	Packet matching criteria based on destination IPv4 address
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-ip
Tree	destination-ip
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-ip address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask *string*

Description	Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-ip mask <i>string</i>
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix *string*

Description	Match a packet if its destination IP address is within the specified IPv4 prefix.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-ip prefix <i>string</i>
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port
Tree	destination-port
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

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

range

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

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl ipv4-filter name string entry sequence-id number match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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

-
- ccs0-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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
 BFDD 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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

value (*number* | *keyword*)

Description	A destination port number
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port value (<i>number</i> <i>keyword</i>)
Tree	value
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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms Supported on all platforms

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

first-fragment *boolean*

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 the more-fragments bit is 1. It is not valid to configure this leaf without configuring a match value for the fragment leaf.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match first-fragment <i>boolean</i>
Tree	first-fragment
Configurable	True
Platforms	Supported on all platforms

fragment *boolean*

Description	Match an IPv4 fragment A packet matches the true condition if the IPv4 header indicates that the fragment-offset is zero 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.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match fragment <i>boolean</i>
Tree	fragment
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match icmp
Tree	icmp
Configurable	True
Platforms	Supported on all platforms

code *number*

Description	Match if the ICMP code value is any value in the list Requires ICMP type to be specified because codes are type dependent.
--------------------	---

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match icmp code <i>number</i>
Tree	code
Configurable	True
Platforms	Supported on all platforms

type (*number* | *keyword*)

Description	Match a single ICMP type value.
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
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
Platforms	Supported on all platforms

protocol (*number* | *keyword*)

Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match protocol (<i>number</i> <i>keyword</i>)
Tree	protocol
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
- ospf
OSPFv2 and OSPFv3
- 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

Platforms

Supported on all platforms

source-ip**Description**

Packet matching criteria based on source IPv4 address

Context[acl ipv4-filter name *string* entry sequence-id *number* match source-ip](#)**Tree**[source-ip](#)**Configurable**

True

Platforms

Supported on all platforms

address string

Description	Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context	acl ipv4-filter name string entry sequence-id number match source-ip address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask string

Description	Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl ipv4-filter name string entry sequence-id number match source-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its source IP address is within the specified IPv4 prefix.
Context	acl ipv4-filter name string entry sequence-id number match source-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl ipv4-filter name string entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

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

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl ipv4-filter name string entry sequence-id number match source-port range
Tree	range
Configurable	True
Platforms	Supported on all platforms

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl ipv4-filter name string entry sequence-id number match source-port range end (number keyword)
Tree	end
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

- rldb
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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl ipv4-filter name string entry sequence-id number match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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)
 - sgmplib
 - 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
	<ul style="list-style-type: none"> • 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
Platforms	Supported on all platforms

value (*number | keyword*)

Description	A source port number
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match source-port value (<i>number keyword</i>)
Tree	value
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
Platforms	Supported on all platforms

tcp-flags *string*

Description	A logical expression using the &, and ! logical operators and the TCP flag names: rst, syn and ack.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> match tcp-flags <i>string</i>
Tree	tcp-flags
Configurable	True

Platforms Supported on all platforms

statistics

Description Container for per-entry statistics

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

Tree [statistics](#)

Configurable False

Platforms Supported on all platforms

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.

Context [acl ipv4-filter name string entry sequence-id number statistics aggregate](#)

Tree [aggregate](#)

Configurable False

Platforms Supported on all platforms

in-last-match *string*

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

Context [acl ipv4-filter name string entry sequence-id number statistics aggregate in-last-match string](#)

Tree [in-last-match](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

in-matched-packets *number*

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

Context [acl ipv4-filter name string entry sequence-id number statistics aggregate in-matched-packets number](#)

Tree [in-matched-packets](#)

Default	0
Configurable	False
Platforms	Supported on all platforms

out-last-match *string*

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
Context	acl ipv4-filter name <i>string</i> entry sequence-id number statistics aggregate out-last-match <i>string</i>
Tree	out-last-match
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

out-matched-packets *number*

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
Context	acl ipv4-filter name <i>string</i> entry sequence-id number statistics aggregate out-matched-packets <i>number</i>
Tree	out-matched-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Time of the last clear command performed by the user at this level or a higher level
Context	acl ipv4-filter name <i>string</i> entry sequence-id number statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

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.
Context	acl ipv4-filter name string entry sequence-id number statistics per-interface
Tree	per-interface
Configurable	False
Platforms	Supported on all platforms

subinterface [name string](#)

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

name [string](#)

Description	Reference to a subinterface.
Context	acl ipv4-filter name string entry sequence-id number statistics per-interface subinterface name string
Configurable	False
Platforms	Supported on all platforms

in-last-match [string](#)

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
Context	acl ipv4-filter name string entry sequence-id number statistics per-interface subinterface name string in-last-match string

Tree	in-last-match
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

in-matched-packets *number*

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
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
Default	0
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Time of the last clear command performed by the user at this level or a higher level
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

out-last-match *string*

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
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

out-matched-packets *number*

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
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
Default	0
Configurable	False
Platforms	Supported on all platforms

tcam-entries

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

linecard [slot](#) *number*

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

slot *number*

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

input-total *number*

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.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot number input-total <i>number</i>
Tree	input-total
Configurable	False
Platforms	Supported on all platforms

output-total *number*

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.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot number output-total <i>number</i>
Tree	output-total
Configurable	False
Platforms	Supported on all platforms

single-instance *number*

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.
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> tcam-entries linecard slot number single-instance <i>number</i>
Tree	single-instance
Configurable	False

Platforms Supported on all platforms

last-clear *string*

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

Context [acl ipv4-filter name](#) *string last-clear string*

Tree [last-clear](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

statistics-per-entry *boolean*

Description Collect statistics for each entry of the ACL
The exact set of statistics depend on the subinterface-specific mode

Context [acl ipv4-filter name](#) *string statistics-per-entry boolean*

Tree [statistics-per-entry](#)

Configurable True

Platforms Supported on all platforms

subinterface-specific *keyword*

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

Context [acl ipv4-filter name](#) *string subinterface-specific keyword*

Tree [subinterface-specific](#)

Default	disabled
Options	<ul style="list-style-type: none"> • disabled • input-only • output-only • input-and-output
Configurable	True
Platforms	Supported on all platforms

ipv6-filter *name string*

Description	List of IPv6 filter policies
Context	acl ipv6-filter name string
Tree	ipv6-filter
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of the IPv6 filter policy.
Context	acl ipv6-filter name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	Description string for the IPv6 filter policy
Context	acl ipv6-filter name string description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

entry *sequence-id number*

Description	List of filter rules.
--------------------	-----------------------

Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Tree	entry
Configurable	True
Platforms	Supported on all platforms

sequence-id *number*

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

action

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

accept

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

log *boolean*

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

Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl ipv6-filter name string entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	Supported on all platforms

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: 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.
Context	acl ipv6-filter name string entry sequence-id number action drop log boolean
Tree	log
Default	false
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	Description string for the filter entry
Context	acl ipv6-filter name string entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	acl ipv6-filter name string entry sequence-id number match
Tree	match
Configurable	True
Platforms	Supported on all platforms

destination-ip

Description	Packet matching criteria based on destination IPv6 address
Context	acl ipv6-filter name string entry sequence-id number match destination-ip
Tree	destination-ip
Configurable	True
Platforms	Supported on all platforms

address string

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl ipv6-filter name string entry sequence-id number match destination-ip address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask string

Description	Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl ipv6-filter name string entry sequence-id number match destination-ip mask string
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Match a packet if its destination IP address is within the specified IPv6 prefix.
Context	acl ipv6-filter name string entry sequence-id number match destination-ip prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl ipv6-filter name string entry sequence-id number match destination-port destination-port
Tree	destination-port
Configurable	True
Platforms	Supported on all platforms

operator keyword

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

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl ipv6-filter name string entry sequence-id number match destination-port range
Tree	range
Configurable	True
Platforms	Supported on all platforms

end (number | keyword)

Description	The ending port number to include in the range
Context	acl ipv6-filter name string entry sequence-id number match destination-port range end (number keyword)
Tree	end
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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl ipv6-filter name string entry sequence-id number match destination-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
Platforms**

True
Supported on all platforms

value (*number* | *keyword*)

Description	A destination port number
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match destination-port value (<i>number</i> <i>keyword</i>)
Tree	value
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl ipv6-filter name string entry sequence-id number match icmp6
Tree	icmp6
Configurable	True
Platforms	Supported on all platforms

code number

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

type (number | keyword)

Description	Match a single ICMPv6 type value
Context	acl ipv6-filter name string entry sequence-id number match icmp6 type (number keyword)

Tree	type
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

	<ul style="list-style-type: none"> • Multicast Listener Discovery Version 2
	<ul style="list-style-type: none"> • mcast-rtr-adv
	Multicast Router Advertisement
	<ul style="list-style-type: none"> • mcast-rtr-solicit
	Multicast Router Solicitation
	<ul style="list-style-type: none"> • mcast-rtr-term
	Multicast Router Termination
Configurable	True
Platforms	Supported on all platforms

next-header (*number* | *keyword*)

Description	An IPv6 packet matches this condition if its first next-header field (in the IPv6 fixed header) contains the specified value
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match next-header (<i>number</i> <i>keyword</i>)
Tree	next-header
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
- ospf
 - OSPFv2 and OSPFv3
- 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
Platforms**

True
Supported on all platforms

source-ip

Description	Packet matching criteria based on source IPv6 address
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-ip
Tree	source-ip
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-ip address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms

mask *string*

Description	Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-ip mask <i>string</i>
Tree	mask
Configurable	True
Platforms	Supported on all platforms

prefix *string*

Description	Match a packet if its source IP address is within the specified IPv6 prefix.
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-ip prefix <i>string</i>
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

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.
Context	acl ipv6-filter name string entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

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

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl ipv6-filter name string entry sequence-id number match source-port range
Tree	range
Configurable	True
Platforms	Supported on all platforms

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl ipv6-filter name string entry sequence-id number match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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

-
- ccs0-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
Platforms	Supported on all platforms

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl ipv6-filter name string entry sequence-id number match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
 BFDD 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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	Supported on all platforms

value (*number* | *keyword*)

Description	A source port number
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> match source-port <i>value</i> (<i>number</i> <i>keyword</i>)
Tree	value
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

- rldb
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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms Supported on all platforms

tcp-flags *string*

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

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

Tree [tcp-flags](#)

Configurable True

Platforms Supported on all platforms

statistics

Description Container for per-entry statistics

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

Tree [statistics](#)

Configurable False

Platforms Supported on all platforms

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.

Context [acl ipv6-filter name string entry sequence-id number statistics aggregate](#)

Tree [aggregate](#)

Configurable False

Platforms Supported on all platforms

in-last-match *string*

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

Context [acl ipv6-filter name string entry sequence-id number statistics aggregate in-last-match string](#)

Tree [in-last-match](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

in-matched-packets *number*

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

Context [acl ipv6-filter name](#) *string* [entry sequence-id](#) *number* [statistics aggregate in-matched-packets](#) *number*

Tree [in-matched-packets](#)

Default 0

Configurable False

Platforms Supported on all platforms

out-last-match *string*

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

Context [acl ipv6-filter name](#) *string* [entry sequence-id](#) *number* [statistics aggregate out-last-match](#) *string*

Tree [out-last-match](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

out-matched-packets *number*

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

Context [acl ipv6-filter name](#) *string* [entry sequence-id](#) *number* [statistics aggregate out-matched-packets](#) *number*

Tree [out-matched-packets](#)

Default 0

Configurable False

Platforms Supported on all platforms

last-clear *string*

Description	Time of the last clear command performed by the user at this level or a higher level
Context	acl ipv6-filter name <i>string</i> entry sequence-id number statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

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.
Context	acl ipv6-filter name <i>string</i> entry sequence-id number statistics per-interface
Tree	per-interface
Configurable	False
Platforms	Supported on all platforms

subinterface *name string*

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

name *string*

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

Configurable	False
Platforms	Supported on all platforms

in-last-match *string*

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
Context	acl ipv6-filter name string entry sequence-id number statistics per-interface subinterface name string in-last-match string
Tree	in-last-match
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

in-matched-packets *number*

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
Context	acl ipv6-filter name string entry sequence-id number statistics per-interface subinterface name string in-matched-packets number
Tree	in-matched-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Time of the last clear command performed by the user at this level or a higher level
Context	acl ipv6-filter name string entry sequence-id number statistics per-interface subinterface name string last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

out-last-match *string*

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
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

out-matched-packets *number*

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
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
Default	0
Configurable	False
Platforms	Supported on all platforms

tcam-entries

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

linecard [slot](#) *number*

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

Platforms Supported on all platforms

slot *number*

Description Slot identifier

Context [acl ipv6-filter name](#) *string* [entry sequence-id](#) *number* [tcam-entries](#) [linecard slot number](#)

Range 1 to 10

Configurable False

Platforms Supported on all platforms

input-total *number*

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.

Context [acl ipv6-filter name](#) *string* [entry sequence-id](#) *number* [tcam-entries](#) [linecard slot number](#) [input-total](#) *number*

Tree [input-total](#)

Configurable False

Platforms Supported on all platforms

output-total *number*

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.

Context [acl ipv6-filter name](#) *string* [entry sequence-id](#) *number* [tcam-entries](#) [linecard slot number](#) [output-total](#) *number*

Tree [output-total](#)

Configurable False

Platforms Supported on all platforms

single-instance *number*

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.
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
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl ipv6-filter name <i>string</i> last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

statistics-per-entry *boolean*

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

subinterface-specific *keyword*

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

Context	<code>acl ipv6-filter name string subinterface-specific keyword</code>
Tree	<code>subinterface-specific</code>
Default	disabled
Options	<ul style="list-style-type: none"> • disabled • input-only • output-only • input-and-output
Configurable	True
Platforms	Supported on all platforms

`mac-filter name string`

Description	List of MAC ACL policies
Context	<code>acl mac-filter name string</code>
Tree	<code>mac-filter</code>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

`name string`

Description	Name of the MAC ACL policy.
Context	<code>acl mac-filter name string</code>
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description *string*

Description	Description string for the MAC ACL policy
Context	acl mac-filter name <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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

Description	List of filter rules.
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i>
Tree	entry
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

sequence-id *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i>
Range	1 to 65535
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action

Description	Container for the actions to be applied to packets matching the filter entry.
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> action
Tree	action
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

accept

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

Tree	accept
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl mac-filter name string entry sequence-id number action accept log boolean
Tree	log
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl mac-filter name string entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information: 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.
Context	acl mac-filter name string entry sequence-id number action drop log boolean
Tree	log
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description string

Description	Description string for the filter entry
Context	acl mac-filter name string entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

match

Description	Container for the conditions that determine whether an Ethernet frame matches this entry
Context	acl mac-filter name string entry sequence-id number match
Tree	match
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-mac

Description	Ethernet frame matching criteria based on destination MAC address
Context	acl mac-filter name string entry sequence-id number match destination-mac
Tree	destination-mac
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Match an Ethernet frame if its destination MAC address logically anded with the mask equals this MAC address.
Context	acl mac-filter name string entry sequence-id number match destination-mac address string
Tree	address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask string

Description	Match an Ethernet frame if its destination MAC address logically anded with the mask equals the configured MAC address.
Context	acl mac-filter name string entry sequence-id number match destination-mac mask string
Tree	mask
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ethertype (string | keyword)

Description	An Ethernet frame matches this condition if its ethertype value (after 802.1Q VLAN tags) matches the specified value
Context	acl mac-filter name string entry sequence-id number match ethertype (string keyword)
Tree	ethertype
Options	<ul style="list-style-type: none"> • <code>ipv4</code> Internet Protocol version 4. Ethertype 0x0800. • <code>arp</code> Address Resolution Protocol. Ethertype 0x0806. • <code>ipv6</code> Internet Protocol version 6. Ethertype 0x86DD. • <code>flow-control</code> Ethernet flow control PAUSE frames. Ethertype 0x8808 • <code>lacp</code> LACP. Ethertype 0x8809. • <code>mpls-unicast</code> MPLS unicast. Ethertype 0x8847. • <code>mpls-multicast</code> MPLS multicast. Ethertype 0x8848. • <code>pppoe-discovery</code> PPPoE discovery. Ethertype 0x8863. • <code>pppoe-session</code> PPPoE session. Ethertype 0x8864. • <code>8021x-authentication</code> 802.1x authentication (EAP). Ethertype 0x888E. • <code>lldp</code> Link Layer Discovery Protocol. Ethertype 0x88CC.

- **macsec**
IEEE 802.1AE MAC security. Ethertype 0x88E5.
- **pbb**
Provider Backbone Bridging. Ethertype 0x88E7.
- **ptp**
Precision Time Protocol. Ethertype 0x88F7.
- **eth-oam**
IEEE 802.1ag CFM and ITU-T Y.1731 OAM. Ethertype 0x8902.
- **fcoe**
Fibre Channel over Ethernet. Ethertype 0x8906.
- **fcoe-initialization**
Fibre Channel over Ethernet Initialization Protocol. Ethertype 0x8914.
- **roce**
RDMA over Converged Ethernet. Ethertype 0x8915.

Configurable

True

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

source-mac**Description**

Ethernet frame matching criteria based on source MAC address

Context[acl mac-filter name string entry sequence-id number match source-mac](#)**Tree**[source-mac](#)**Configurable**

True

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string**Description**

Match an Ethernet frame if its source MAC address logically anded with the mask equals this MAC address.

Context[acl mac-filter name string entry sequence-id number match source-mac address string](#)**Tree**[address](#)**Configurable**

True

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask string

Description	Match an Ethernet frame if its source MAC address logically anded with the mask equals the configured MAC address.
Context	acl mac-filter name string entry sequence-id number match source-mac mask string
Tree	mask
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

vlan

Description	Ethernet frame matching criteria based on VLAN tags
Context	acl mac-filter name string entry sequence-id number match vlan
Tree	vlan
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

outermost-vlan-id

Description	Ethernet frame matching criteria based on the outermost VLAN ID found before the subinterface-defining VLAN tag (if any) is removed.
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id
Tree	outermost-vlan-id
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

none

Description	When configured, only untagged frames are matched.
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id none
Tree	none
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

operator *keyword*

Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id operator keyword
Tree	operator
Options	<ul style="list-style-type: none"> le Less than or equal. ge Greater than or equal. eq Equal to.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

range

Description	Container used to specify a contiguous range of VLAN IDs. Matched values include the start and end values.
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id range
Tree	range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

end *number*

Description	The ending VLAN ID to include in the range
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id range end number
Tree	end
Range	0 to 4095
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

start number

Description	The starting VLAN ID to include in the range
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id range start number
Tree	start
Range	0 to 4095
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

value number

Description	A VLAN ID number A value of zero is used to match priority-tagged 802.1Q frames.
Context	acl mac-filter name string entry sequence-id number match vlan outermost-vlan-id value number
Tree	value
Range	0 to 4095
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description	Container for per-entry statistics
Context	acl mac-filter name string entry sequence-id number statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl mac-filter name string entry sequence-id number statistics aggregate
Tree	aggregate
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-last-match *string*

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
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate in-last-match <i>string</i>
Tree	in-last-match
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-matched-packets *number*

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
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate in-matched-packets <i>number</i>
Tree	in-matched-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

out-last-match *string*

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
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate out-last-match <i>string</i>
Tree	out-last-match
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

out-matched-packets *number*

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
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics aggregate out-matched-packets <i>number</i>
Tree	out-matched-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Time of the last clear command performed by the user at this level or a higher level
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

subinterface *name string*

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.

Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

name *string*

Description	Reference to a subinterface.
Context	acl mac-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-last-match *string*

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
Context	acl mac-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
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-matched-packets *number*

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
Context	acl mac-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
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Time of the last clear command performed by the user at this level or a higher level
Context	acl mac-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
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

out-last-match *string*

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
Context	acl mac-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
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

out-matched-packets *number*

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
Context	acl mac-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
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcam-entries

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

Tree	tcam-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

linecard *slot number*

Description	List of linecards in the system
Context	acl mac-filter name string entry sequence-id number tcam-entries linecard slot number
Tree	linecard
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

slot *number*

Description	Slot identifier
Context	acl mac-filter name string entry sequence-id number tcam-entries linecard slot number
Range	1 to 10
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

input-total *number*

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>
Context	acl mac-filter name string entry sequence-id number tcam-entries linecard slot number input-total number
Tree	input-total
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

output-total *number*

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.
Context	acl mac-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
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

single-instance *number*

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.
Context	acl mac-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
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Time of the last clear command performed by the user at this level
Context	acl mac-filter name <i>string</i> last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics-per-entry *boolean*

Description	Collect statistics for each entry of the ACL
--------------------	--

	The exact set of statistics depend on the subinterface-specific mode
Context	<code>acl mac-filter name string statistics-per-entry boolean</code>
Tree	<code>statistics-per-entry</code>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

subinterface-specific *keyword*

Description	<p>Controls the instantiation of the filter when it is applied as an input or output ACL</p> <p>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</p> <p>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</p> <p>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</p> <p>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</p>
Context	<code>acl mac-filter name string subinterface-specific keyword</code>
Tree	<code>subinterface-specific</code>
Default	disabled
Options	<ul style="list-style-type: none"> • disabled • input-only • output-only • input-and-output
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

policers

Description	Container for policer definitions used by ACL entries
Context	<code>acl policers</code>
Tree	<code>policers</code>
Configurable	True

Platforms Supported on all platforms

policer *name string*

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.

Context [acl policers policer name string](#)

Tree [policer](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

name *string*

Description User-defined name of the policer

Context [acl policers policer name string](#)

String Length 1 to 255

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

entry-specific *boolean*

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.

Context [acl policers policer name string entry-specific boolean](#)

Tree [entry-specific](#)

Default false

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

max-burst *number*

Description The MBS bucket depth in bytes

Context [acl policers policer name string max-burst number](#)

Tree	max-burst
Range	1 to 125000000
Units	bytes
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

peak-rate *number*

Description	The PIR rate in kbps (bucket empty/fill rate).
Context	acl policers policer name <i>string</i> peak-rate number
Tree	peak-rate
Range	1 to 1000000
Units	kbps
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description	Container for linecard policer statistics None of these statistics are populated if the policer is configured as entry-specific=true.
Context	acl policers policer name <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-octets *number*

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.
Context	acl policers policer name <i>string</i> statistics conforming-octets number
Tree	conforming-octets
Default	0
Configurable	False

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

conforming-packets *number*

Description The number of packets (actually Ethernet frames) that were considered conforming by the policer

Context [acl policers policer name string statistics conforming-packets number](#)

Tree [conforming-packets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-octets *number*

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.

Context [acl policers policer name string statistics exceeding-octets number](#)

Tree [exceeding-octets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

exceeding-packets *number*

Description The number of packets (actually Ethernet frames) that were considered exceeding by the policer

Context [acl policers policer name string statistics exceeding-packets number](#)

Tree [exceeding-packets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description Time of the last clear command that applied to these statistics

Context	<code>acl policers policer name string statistics last-clear string</code>
Tree	<code>last-clear</code>
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

system-cpu-policer `name string`

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.
Context	<code>acl policers system-cpu-policer name string</code>
Tree	<code>system-cpu-policer</code>
Configurable	True
Platforms	Supported on all platforms

name `string`

Description	User-defined name of the policer
Context	<code>acl policers system-cpu-policer name string</code>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

entry-specific `boolean`

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.
Context	<code>acl policers system-cpu-policer name string entry-specific boolean</code>
Tree	<code>entry-specific</code>
Default	false
Configurable	True
Platforms	Supported on all platforms

max-packet-burst *number*

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

peak-packet-rate *number*

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

statistics

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

conforming-octets *number*

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.
Context	acl policers system-cpu-policer name <i>string</i> statistics conforming-octets <i>number</i>
Tree	conforming-octets
Default	0

Configurable	False
Platforms	Supported on all platforms

conforming-packets *number*

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

exceeding-octets *number*

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.
Context	acl policers system-cpu-policer name <i>string</i> statistics exceeding-octets number
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

exceeding-packets *number*

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

last-clear *string*

Description	Time of the last clear command that applied to these statistics
Context	acl policers system-cpu-policer name <i>string</i> statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

system-filter

Description	Top level container for System filters
Context	acl system-filter
Tree	system-filter
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ipv4-filter

Description	Top level container for System IPv4 filters
Context	acl system-filter ipv4-filter
Tree	ipv4-filter
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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

Description	List of filter rules.
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i>
Tree	entry
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

sequence-id *number*

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

Range	1 to 256
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action

Description	Container for the actions to be applied to packets matching the System filter entry.
Context	acl system-filter ipv4-filter entry sequence-id number action
Tree	action
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

accept

Description	Accept matching packets
Context	acl system-filter ipv4-filter entry sequence-id number action accept
Tree	accept
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl system-filter ipv4-filter entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

log *boolean*

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

Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description string

Description	Description string for the filter entry
Context	acl system-filter ipv4-filter entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	acl system-filter ipv4-filter entry sequence-id number match
Tree	match
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-ip

Description	Packet matching criteria based on destination IPv4 address
Context	acl system-filter ipv4-filter entry sequence-id number match destination-ip
Tree	destination-ip
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.
Context	acl system-filter ipv4-filter entry sequence-id number match destination-ip address string
Tree	address
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask *string*

Description Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.

Context [acl system-filter ipv4-filter entry sequence-id number match destination-ip mask string](#)

Tree [mask](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

prefix *string*

Description Match a packet if its destination IP address is within the specified IPv4 prefix.

Context [acl system-filter ipv4-filter entry sequence-id number match destination-ip prefix string](#)

Tree [prefix](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.

Context [acl system-filter ipv4-filter entry sequence-id number match destination-port](#)

Tree [destination-port](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

operator *keyword*

Description Comparison operator
eq = equal ge = greater than or equal to le = less than or equal to

Context [acl system-filter ipv4-filter entry sequence-id number match destination-port operator keyword](#)

Tree	operator
Options	<ul style="list-style-type: none"> • <code>le</code> Less than or equal. • <code>ge</code> Greater than or equal. • <code>eq</code> Equal to.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl system-filter ipv4-filter entry sequence-id number match destination-port range
Tree	range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl system-filter ipv4-filter entry sequence-id number match destination-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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

-
- 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)
- `tcpnethaspsrv`
`tcpnethaspsrv`, 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

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

start (*number* | *keyword*)

Description The starting port number to include in the range

Context [acl system-filter ipv4-filter entry sequence-id](#) *number* [match destination-port range start](#) (*number* | *keyword*)

Tree	start
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)
 - sgmpp
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)
- tcpnethaspsrv
tcpnethaspsrv, 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
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

value (*number* | *keyword*)

Description	A destination port number
Context	acl system-filter ipv4-filter entry sequence-id number match destination-port value (number keyword)
Tree	value
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
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

first-fragment *boolean*

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.
Context	acl system-filter ipv4-filter entry sequence-id number match first-fragment boolean
Tree	first-fragment
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

fragment *boolean*

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.
--------------------	---

Context	acl system-filter ipv4-filter entry sequence-id number match fragment <i>boolean</i>
Tree	fragment
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl system-filter ipv4-filter entry sequence-id number match icmp
Tree	icmp
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

code *number*

Description	Match if the ICMP code value is any value in the list Requires ICMP type to be specified because codes are type dependent.
Context	acl system-filter ipv4-filter entry sequence-id number match icmp code number
Tree	code
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

type (*number* | *keyword*)

Description	Match a single ICMP type value.
Context	acl system-filter ipv4-filter entry sequence-id number match icmp type (number keyword)
Tree	type
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

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

protocol (*number* | *keyword*)**Description**

An IPv4 packet matches this condition if its IP protocol type field matches the specified value

Context[acl system-filter ipv4-filter entry sequence-id](#) *number* [match protocol](#) (*number* | *keyword*)**Tree**[protocol](#)**Range**

0 to 255

Options

- 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
- ospf
OSPFv2 and OSPFv3
- 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

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

source-ip

Description Packet matching criteria based on source IPv4 address

Context [acl system-filter ipv4-filter entry sequence-id number match source-ip](#)

Tree [source-ip](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.

Context [acl system-filter ipv4-filter entry sequence-id number match source-ip address string](#)

Tree [address](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask string

Description Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.

Context [acl system-filter ipv4-filter entry sequence-id number match source-ip mask string](#)

Tree [mask](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

prefix *string*

Description Match a packet if its source IP address is within the specified IPv4 prefix.

Context [acl system-filter ipv4-filter entry sequence-id number match source-ip prefix string](#)

Tree [prefix](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.

Context [acl system-filter ipv4-filter entry sequence-id number match source-port](#)

Tree [source-port](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

operator *keyword*

Description Comparison operator

eq = equal ge = greater than or equal to le = less than or equal to

Context [acl system-filter ipv4-filter entry sequence-id number match source-port operator keyword](#)

Tree [operator](#)

- Options**
- le
Less than or equal.
 - ge
Greater than or equal.
 - eq
Equal to.

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl system-filter ipv4-filter entry sequence-id number match source-port range
Tree	range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

end (number | keyword)

Description	The ending port number to include in the range
Context	acl system-filter ipv4-filter entry sequence-id number match source-port range end (number keyword)
Tree	end
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

- 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

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

start (*number* | *keyword*)**Description**

The starting port number to include in the range

Context[acl system-filter ipv4-filter entry sequence-id number match source-port range start](#) (*number* | *keyword*)**Tree**[start](#)**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

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

value (*number* | *keyword*)

Description	A source port number
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i> match source-port value (<i>number</i> <i>keyword</i>)
Tree	value
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
 - BFDD 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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcp-flags *string*

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

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

Tree [tcp-flags](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description Statistics container for packets matching the system-filter entry

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

Tree [statistics](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

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

Context [acl system-filter ipv4-filter entry sequence-id number statistics last-clear string](#)

Tree [last-clear](#)

String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-match string

Description	The elapsed time since a packet last matched the entry, considering all subinterfaces.
Context	acl system-filter ipv4-filter entry sequence-id number statistics last-match string
Tree	last-match
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

matched-packets number

Description	The number of packets matching the entry since it was programmed or since the last clear, summed across all subinterfaces
Context	acl system-filter ipv4-filter entry sequence-id number statistics matched-packets number
Tree	matched-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcam-entries number

Description	The number of TCAM entries required to implement a single instance of this filter rule.
Context	acl system-filter ipv4-filter entry sequence-id number tcam-entries number
Tree	tcam-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear string

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

Context	acl system-filter ipv4-filter last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ipv6-filter

Description	Top level container for System IPv6 filters
Context	acl system-filter ipv6-filter
Tree	ipv6-filter
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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

Description	List of filter rules.
Context	acl system-filter ipv6-filter entry sequence-id <i>number</i>
Tree	entry
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

[sequence-id](#) *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl system-filter ipv6-filter entry sequence-id <i>number</i>
Range	1 to 128
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action

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

Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

accept

Description	Accept matching packets
Context	acl system-filter ipv6-filter entry sequence-id number action accept
Tree	accept
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

drop

Description	Drop matching packets without sending any ICMP messages back to the source
Context	acl system-filter ipv6-filter entry sequence-id number action drop
Tree	drop
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

log *boolean*

Description	When this is true, a log is created for each packet matching the entry The log entry contains the following information:
Context	acl system-filter ipv6-filter entry sequence-id number action drop log boolean
Tree	log
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description *string*

Description	Description string for the filter entry
Context	acl system-filter ipv6-filter entry sequence-id number description string
Tree	description
String Length	1 to 255
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

match

Description Container for the conditions that determine whether a packet matches this entry

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

Tree [match](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-ip

Description Packet matching criteria based on destination IPv6 address

Context [acl system-filter ipv6-filter entry sequence-id number match destination-ip](#)

Tree [destination-ip](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address *string*

Description Match a packet if its destination IP address logically anded with the inverse of the mask equals this IP address.

Context [acl system-filter ipv6-filter entry sequence-id number match destination-ip address string](#)

Tree [address](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask *string*

Description Match a packet if its destination IP address logically anded with the inverse of this mask equals the configured IP address.

Context [acl system-filter ipv6-filter entry sequence-id number match destination-ip mask string](#)

Tree [mask](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

prefix string

Description	Match a packet if its destination IP address is within the specified IPv6 prefix.
Context	acl system-filter ipv6-filter entry sequence-id number match destination-ip prefix string
Tree	prefix
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl system-filter ipv6-filter entry sequence-id number match destination-port destination-port
Tree	destination-port
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

operator keyword

Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Context	acl system-filter ipv6-filter entry sequence-id number match destination-port operator keyword
Tree	operator
Options	<ul style="list-style-type: none"> • le Less than or equal. • ge Greater than or equal. • eq Equal to.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl system-filter ipv6-filter entry sequence-id number match destination-port range
Tree	range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl system-filter ipv6-filter entry sequence-id number match destination-port range end (number keyword)
Tree	end
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

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

start (*number* | *keyword*)**Description**

The starting port number to include in the range

Context[acl system-filter ipv6-filter entry sequence-id number match destination-port range start](#) (*number* | *keyword*)**Tree**[start](#)**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)
- sgmplib
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

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

value (*number* | *keyword*)

Description	A destination port number
Context	acl system-filter ipv6-filter entry sequence-id <i>number</i> match destination-port value (<i>number</i> <i>keyword</i>)
Tree	value
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)
- tcpnethaspsrv
tcpnethaspsrv, Aladdin Knowledge Systems Hasp services
- tftp
Trivial File Transfer Protocol (TFTP)
- time
Time Protocol
- timed
Timeserver
- ups

	Uninterruptible power supply (UPS)
	<ul style="list-style-type: none"> • 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
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dscp-set (*number* | *keyword*)

Description	A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.
Context	acl system-filter ipv6-filter entry sequence-id <i>number</i> match dscp-set (<i>number</i> <i>keyword</i>)
Tree	dscp-set
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
Platforms	7220 IXR-D2L, 7250 IXR-10, 7250 IXR-6, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl system-filter ipv6-filter entry sequence-id number match icmp6
Tree	icmp6
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

code number

Description	Match if the ICMPv6 code value is any value in the list Requires ICMPv6 type to be specified because codes are type dependent.
Context	acl system-filter ipv6-filter entry sequence-id number match icmp6 code number
Tree	code
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

type (number | keyword)

Description	Match a single ICMPv6 type value
Context	acl system-filter ipv6-filter entry sequence-id number match icmp6 type (number keyword)

Tree	type
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
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

next-header (*number* | *keyword*)

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

- 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
- ospf
 - OSPFv2 and OSPFv3
- 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

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

source-ip

Description	Packet matching criteria based on source IPv6 address
Context	acl system-filter ipv6-filter entry sequence-id number match source-ip
Tree	source-ip
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Match a packet if its source IP address logically anded with the inverse of the mask equals this IP address.
Context	acl system-filter ipv6-filter entry sequence-id number match source-ip address string
Tree	address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mask string

Description	Match a packet if its source IP address logically anded with the inverse of this mask equals the configured IP address.
Context	acl system-filter ipv6-filter entry sequence-id number match source-ip mask string
Tree	mask
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

prefix string

Description	Match a packet if its source IP address is within the specified IPv6 prefix.
Context	acl system-filter ipv6-filter entry sequence-id number match source-ip prefix string
Tree	prefix
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

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.
Context	acl system-filter ipv6-filter entry sequence-id number match source-port
Tree	source-port
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

operator *keyword*

Description	Comparison operator eq = equal ge = greater than or equal to le = less than or equal to
Context	acl system-filter ipv6-filter entry sequence-id number match source-port operator keyword
Tree	operator
Options	<ul style="list-style-type: none"> • le Less than or equal. • ge Greater than or equal. • eq Equal to.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

range

Description	Container used to specify a contiguous range of TCP/UDP port numbers
Context	acl system-filter ipv6-filter entry sequence-id number match source-port range
Tree	range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

end (*number* | *keyword*)

Description	The ending port number to include in the range
Context	acl system-filter ipv6-filter entry sequence-id number match source-port range end (<i>number</i> <i>keyword</i>)
Tree	end
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

- ccs0-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
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

start (*number* | *keyword*)

Description	The starting port number to include in the range
Context	acl system-filter ipv6-filter entry sequence-id <i>number</i> match source-port range start (<i>number</i> <i>keyword</i>)
Tree	start
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
 BFDD 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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

value (*number* | *keyword*)

Description A source port number

Context [acl system-filter ipv6-filter entry sequence-id number match source-port value](#) (*number* | *keyword*)

Tree [value](#)

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
- 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

- rldb
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)
- sgmplib
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)
- tcpnethaspsrv
tcpnethaspsrv, 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

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcp-flags *string*

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

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

Tree [tcp-flags](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description Statistics container for packets matching the system-filter entry

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

Tree [statistics](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

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

Context [acl system-filter ipv6-filter entry sequence-id number statistics last-clear string](#)

Tree [last-clear](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-match *string*

Description The elapsed time since a packet last matched the entry, considering all subinterfaces.

Context [acl system-filter ipv6-filter entry sequence-id number statistics last-match string](#)

Tree [last-match](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

matched-packets *number*

Description The number of packets matching the entry since it was programmed or since the last clear, summed across all subinterfaces

Context [acl system-filter ipv6-filter entry sequence-id number statistics matched-packets number](#)

Tree [matched-packets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcam-entries *number*

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

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

Tree [tcam-entries](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

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

Context [acl system-filter ipv6-filter last-clear string](#)

Tree [last-clear](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tcam-profile *keyword*

Description Specify the TCAM resource management profile

Context [acl tcam-profile keyword](#)

Tree [tcam-profile](#)

Options

- default

	Default allocation that provides twice as many resources to ingress ACLs as egress ACLs
	<ul style="list-style-type: none">• ipv4-egress-scaled
	Alternate allocation that provides more resources to IPv4 egress ACLs than any other application
	<ul style="list-style-type: none">• ipv4-pbf-scaled
	Alternate allocation that provides more resources for IPv4 policy-forwarding rules
Configurable	True
Platforms	Supported on all platforms

4 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
- ipv6-link-local-interface string
- 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
```

4.1 bfd Descriptions

bfd

Description	Context to configure BFD parameters and report BFD sessions state
Context	bfd
Tree	bfd
Configurable	True
Platforms	Supported on all platforms

micro-bfd-sessions

Description	Context to configure micro-BFD session parameters and report sessions state
Context	bfd micro-bfd-sessions
Tree	micro-bfd-sessions
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lag-interface [name reference](#)

Description	List of ethernet interface references to associate a micro-BFD session config and state
Context	bfd micro-bfd-sessions lag-interface name reference
Tree	lag-interface
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name [reference](#)

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

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description Administratively enable or disable BFD for this subinterface

Context [bfd micro-bfd-sessions lag-interface name](#) *reference* [admin-state](#) *keyword*

Tree [admin-state](#)

Default disable

Options

- enable
- disable

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

desired-minimum-transmit-interval *number*

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.

Context [bfd micro-bfd-sessions lag-interface name](#) *reference* [desired-minimum-transmit-interval](#) *number*

Tree [desired-minimum-transmit-interval](#)

Range 10000 to 100000000

Default 1000000

Units microseconds

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

detection-multiplier *number*

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.

Context [bfd micro-bfd-sessions lag-interface name](#) *reference* [detection-multiplier](#) *number*

Tree	detection-multiplier
Range	3 to 20
Default	3
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

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

Description	IP address to be used as source address in BFD packets
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> local-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	local-address
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

member-interface *name string*

Description	List of ethernet interface references to associate a micro-BFD session config and state
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name string
Tree	member-interface
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *string*

Description	Reference ID for associated ethernet interface Example: ethernet-2/1 (Reference Interface ethernet-2/1).
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name string
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

active-receive-interval *number*

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.
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> active-receive-interval <i>number</i>
Tree	active-receive-interval
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

active-transmit-interval *number*

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
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> active-transmit-interval <i>number</i>
Tree	active-transmit-interval
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

async

Description	Container for async BFD operational state parameters
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> async
Tree	async
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-clear *string*

Description	Timestamp of the last time the session counters were cleared.
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

String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-packet-received *string*

Description	Timestamp for when the last BFD packet was received for this session
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
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-packet-transmitted *string*

Description	Timestamp for when the last BFD packet was transmitted for this session
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
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

received-errored-packets *number*

Description	Counter for the number of BFD packets received with BFD level errors
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
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

received-packets *number*

Description	Counter for the number of BFD packets received for this session
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string async received-packets number</i>
Tree	received-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

transmitted-packets *number*

Description	Counter for the number of BFD packets transmitted for this session
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string async transmitted-packets number</i>
Tree	transmitted-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

up-transitions *number*

Description	Counter for the number of UP transitions for this BFD session
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string async up-transitions number</i>
Tree	up-transitions
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

failure-transitions *number*

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

Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-failure-time string

Description	Timestamp of the last BFD session transition out of the up state to down state
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> last-failure-time string
Tree	last-failure-time
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-state-transition string

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.
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> last-state-transition string
Tree	last-state-transition
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

local-diagnostic-code keyword

Description	The local BFD diagnostic code indicating the most recent reason for failure of this BFD session
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> local-diagnostic-code keyword
Tree	local-diagnostic-code
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_SIGNALED_DOWN

The neighbor signaled session down

- FORWARDING_RESET

The forwarding plane in the local system was 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

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

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

Platforms

7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

local-discriminator *number*

Description

BFD session local discriminator

Context

[bfd micro-bfd-sessions lag-interface name](#) *reference* [member-interface name string](#) [local-discriminator number](#)

Tree

[local-discriminator](#)

Configurable

False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-control-plane-independent *boolean*

Description Indicates if the remote neighbor has set the control independent flag

Context [bfd micro-bfd-sessions lag-interface name](#) *reference* [member-interface name](#) *string* [remote-control-plane-independent](#) *boolean*

Tree [remote-control-plane-independent](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-diagnostic-code *keyword*

Description The remote BFD diagnostic code indicating the remote system's reason for failure of the BFD session

Context [bfd micro-bfd-sessions lag-interface name](#) *reference* [member-interface name](#) *string* [remote-diagnostic-code](#) *keyword*

Tree [remote-diagnostic-code](#)

Options

- 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 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

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.

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
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-discriminator *number*

Description	A unique identifier used by the remote system to identify this BFD session.
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> remote-discriminator number
Tree	remote-discriminator
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-minimum-receive-interval *number*

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.
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> member-interface name <i>string</i> remote-minimum-receive-interval number
Tree	remote-minimum-receive-interval
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-multiplier *number*

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.
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
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-session-state *keyword*

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.
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
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
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

session-state *keyword*

Description	The state of the BFD session perceived by the local system
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
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
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-address (*ipv4-address* | *ipv6-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.
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> remote-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	remote-address
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

required-minimum-receive *number*

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.
Context	bfd micro-bfd-sessions lag-interface name <i>reference</i> required-minimum-receive <i>number</i>
Tree	required-minimum-receive
Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True

Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
------------------	--

network-instance *name* *string*

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

name *string*

Description	A unique name identifying the network instance
Context	bfd network-instance name <i>string</i>
Configurable	False
Platforms	Supported on all platforms

peer local-discriminator *number*

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

local-discriminator *number*

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

active-receive-interval *number*

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.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> active-receive-interval <i>number</i>
Tree	active-receive-interval
Configurable	False
Platforms	Supported on all platforms

active-transmit-interval *number*

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
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> active-transmit-interval <i>number</i>
Tree	active-transmit-interval
Configurable	False
Platforms	Supported on all platforms

async

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

last-clear *string*

Description	Timestamp of the last time the session counters were cleared.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> async last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-packet-received *string*

Description	Timestamp for when the last BFD packet was received for this session
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-packet-transmitted *string*

Description	Timestamp for when the last BFD packet was transmitted for this session
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

received-errored-packets *number*

Description	Counter for the number of BFD packets received with BFD level errors
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
Default	0
Configurable	False
Platforms	Supported on all platforms

received-packets *number*

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

Platforms Supported on all platforms

transmitted-packets *number*

Description Counter for the number of BFD packets transmitted for this session

Context [bfd network-instance name](#) *string* [peer local-discriminator](#) *number* [async transmitted-packets](#) *number*

Tree [transmitted-packets](#)

Default 0

Configurable False

Platforms Supported on all platforms

up-transitions *number*

Description Counter for the number of UP transitions for this BFD session

Context [bfd network-instance name](#) *string* [peer local-discriminator](#) *number* [async up-transitions](#) *number*

Tree [up-transitions](#)

Default 0

Configurable False

Platforms Supported on all platforms

failure-transitions *number*

Description The number of times that the BFD session has transitioned out of the up state

Context [bfd network-instance name](#) *string* [peer local-discriminator](#) *number* [failure-transitions](#) *number*

Tree [failure-transitions](#)

Configurable False

Platforms Supported on all platforms

ipv6-link-local-interface *string*

Description For IPv6 link local sessions only, indicates the local interface with which the session is associated.

Context [bfd network-instance name](#) *string* [peer local-discriminator](#) *number* [ipv6-link-local-interface](#) *string*

Tree	ipv6-link-local-interface
Configurable	False
Platforms	Supported on all platforms

last-failure-time *string*

Description	Timestamp of the last BFD session transition out of the up state to down state
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> last-failure-time <i>string</i>
Tree	last-failure-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-state-transition *string*

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.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> last-state-transition <i>string</i>
Tree	last-state-transition
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

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

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

local-diagnostic-code *keyword*

Description	The local BFD diagnostic code indicating the most recent reason for failure of this BFD session
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> local-diagnostic-code <i>keyword</i>
Tree	local-diagnostic-code
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 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 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 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

Platforms Supported on all platforms

oper-state *keyword*

Description Details the operational state of the session

Context [bfd network-instance name](#) *string* [peer local-discriminator number](#) [oper-state keyword](#)

Tree [oper-state](#)

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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting

Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

remote-address (*ipv4-address* | *ipv6-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.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	remote-address
Configurable	False
Platforms	Supported on all platforms

remote-control-plane-independent *boolean*

Description	Indicates if the remote neighbor has set the control independent flag
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
Configurable	False
Platforms	Supported on all platforms

remote-diagnostic-code *keyword*

Description	The remote BFD diagnostic code indicating the remote system's reason for failure of the BFD session
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-diagnostic-code <i>keyword</i>
Tree	remote-diagnostic-code
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_SINGALED_DOWN

The neighbor signaled session down

- FORWARDING_RESET

The forwarding plane in the local system was 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

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

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
Platforms	Supported on all platforms

remote-discriminator *number*

Description	A unique identifier used by the remote system to identify this BFD session
Context	bfd network-instance name <i>string</i> peer local-discriminator number remote-discriminator number
Tree	remote-discriminator
Configurable	False
Platforms	Supported on all platforms

remote-minimum-receive-interval *number*

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.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-minimum-receive-interval <i>number</i>
Tree	remote-minimum-receive-interval
Configurable	False
Platforms	Supported on all platforms

remote-multiplier *number*

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.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-multiplier <i>number</i>
Tree	remote-multiplier
Configurable	False
Platforms	Supported on all platforms

remote-session-state *keyword*

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.
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> remote-session-state <i>keyword</i>
Tree	remote-session-state
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
Platforms	Supported on all platforms

session-state *keyword*

Description	The state of the BFD session perceived by the local system
Context	bfd network-instance name <i>string</i> peer local-discriminator <i>number</i> session-state <i>keyword</i>
Tree	session-state
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
Platforms	Supported on all platforms

subscribed-protocols *string*

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

subinterface *id string*

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

id string

Description	Reference ID for associated subinterface Example: ethernet-2/1.100 (Reference Interface ethernet-2/1, subinterface 100).
Context	bfd subinterface id string
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

admin-state keyword

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

desired-minimum-transmit-interval number

Description	<p>The minimum interval between transmission of BFD control packets</p> <p>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.</p>
Context	bfd subinterface id string desired-minimum-transmit-interval number
Tree	desired-minimum-transmit-interval
Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True
Platforms	Supported on all platforms

detection-multiplier *number*

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.
Context	bfd subinterface id <i>string</i> detection-multiplier <i>number</i>
Tree	detection-multiplier
Range	3 to 20
Default	3
Configurable	True
Platforms	Supported on all platforms

minimum-echo-receive-interval *number*

Description	The minimum interval between echo packets the local node can receive Implicitly enabled echo mode on the associated interface.
Context	bfd subinterface id <i>string</i> minimum-echo-receive-interval <i>number</i>
Tree	minimum-echo-receive-interval
Range	0 250000 to 100000000
Default	0
Configurable	True
Platforms	Supported on all platforms

required-minimum-receive *number*

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.
Context	bfd subinterface id <i>string</i> required-minimum-receive <i>number</i>
Tree	required-minimum-receive
Range	10000 to 100000000
Default	1000000
Units	microseconds
Configurable	True
Platforms	Supported on all platforms

total-bfd-sessions *number*

Description	Counter for the total number of BFD sessions
Context	bfd total-bfd-sessions <i>number</i>
Tree	total-bfd-sessions
Default	0
Configurable	False
Platforms	Supported on all platforms

total-unmatched-bfd-packets *number*

Description	Counter for the total number of BFD packets received not matching a BFD session
Context	bfd total-unmatched-bfd-packets <i>number</i>
Tree	total-unmatched-bfd-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

5 interface

```

interface name string
+ admin-state keyword
+ breakout-mode
+ channel-speed keyword
+ num-channels keyword
+ description string
+ ethernet
+ aggregate-id reference
+ auto-negotiate boolean
+ duplex-mode keyword
+ flow-control
+ receive boolean
+ hold-time
+ down number
- down-expires string
+ up number
- up-expires string
- hw-mac-address string
+ l2cp-transparency
+ dot1x
- oper-rule keyword
+ tunnel boolean
+ lacp
- oper-rule keyword
+ tunnel boolean
+ lldp
- oper-rule keyword
+ tunnel boolean
+ ptp
- oper-rule keyword
+ tunnel boolean
+ tunnel-all-l2cp boolean
+ xstp
- oper-rule keyword
+ tunnel boolean
+ lacp-port-priority number
- physical-medium keyword
+ port-speed keyword
+ reload-delay number
- reload-delay-expires string
+ standby-signaling 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
+ storm-control
+ broadcast-rate number
+ multicast-rate number
- operational-broadcast-rate number
- operational-multicast-rate number
- operational-unknown-unicast-rate number
+ units keyword
+ unknown-unicast-rate number
- ifindex number
+ lag
+ lacp
+ admin-key number
+ interval keyword
+ lacp-mode keyword
+ system-id-mac string
+ system-priority number
+ lacp-fallback-mode keyword
+ lacp-fallback-timeout number
- lag-speed number
+ lag-type keyword
- member name reference
- lacp
- activity keyword
- aggregatable boolean
- collecting boolean
- distributing boolean
- lacp-port-priority number
- oper-key number
- 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
- last-change string
- microbfd-enabled boolean
- oper-down-reason keyword
- oper-state keyword
+ member-speed keyword
+ min-links number
- last-change string
+ loopback-mode boolean
+ mtu number
- oper-down-reason keyword
- oper-state keyword
+ qos
+ output
+ multicast-queue queue-id number
- forwarding-class keyword
- queue-depth
- last-high-threshold-time string
- maximum-burst-size number
+ scheduling

```

```

- peak-rate-bps number
+ peak-rate-percent number
- scheduler-node reference
+ template reference
+ scheduler
+ tier level number
+ node node-number number
+ strict-priority boolean
+ weight number
+ unicast-queue queue-id number
- active-queue-management
- ecn-slope ecn-drop-probability keyword
- max-probability number
- max-threshold-bytes number
- min-threshold-bytes number
- slope-enabled boolean
- wred-slope traffic-type keyword drop-probability keyword
- max-probability number
- max-threshold-bytes number
- min-threshold-bytes number
- slope-enabled boolean
- forwarding-class keyword
- queue-depth
- high-threshold-bytes number
- last-high-threshold-time string
- maximum-burst-size number
+ scheduling
- peak-rate-bps number
+ peak-rate-percent number
- scheduler-node reference
+ strict-priority boolean
+ weight number
+ template reference
+ voq-template reference
- 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
- high-drop-probability number
- low-drop-probability number
- medium-drop-probability number
- dropped-packets
- high-drop-probability number
- low-drop-probability number
- medium-drop-probability number
- forwarded-octets
- high-drop-probability number
- low-drop-probability number
- medium-drop-probability number
- forwarded-packets
- high-drop-probability number
- low-drop-probability number
- medium-drop-probability number
- queue-depth
- high-threshold-bytes number

```

```

- last-high-threshold-time string
+ sflow
+ admin-state keyword
- statistics
- carrier-transitions number
- in-broadcast-packets number
- in-discarded-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-discarded-packets number
- out-error-packets number
- out-mirror-octets number
- out-mirror-packets number
- out-multicast-packets number
- out-octets number
- out-unicast-packets number
+ subinterface index number
+ acl
+ input
+ ipv4-filter reference
+ ipv6-filter reference
+ mac-filter reference
+ output
+ ipv4-filter reference
+ ipv6-filter reference
+ mac-filter reference
+ admin-state keyword
+ anycast-gw
+ anycast-gw-mac string
- anycast-gw-mac-origin keyword
+ virtual-router-id number
+ bridge-table
+ discard-unknown-src-mac boolean
+ mac-duplication
+ action keyword
- duplicate-entries
- mac address string
- dup-detect-time string
- hold-down-time-remaining (keyword | number)
+ mac-learning
+ admin-state keyword
+ aging
+ admin-state keyword
- learnt-entries
- mac address string
- aging (number | keyword)
- last-update string
+ mac-limit
+ maximum-entries number
+ warning-threshold-pct number
- mac-table
- mac address string
- failed-slots number
- last-update string
- not-programmed-reason keyword
- type keyword
- statistics
- active-entries number
- failed-entries number
- mac-type type keyword
- active-entries number

```

```

    - failed-entries number
    - total-entries number
  - total-entries number
+ description string
- ethernet-segment-association
  - designated-forwarder boolean
  - es-managed boolean
  - ethernet-segment string
- ifindex number
+ ip-mtu number
+ ipv4
  + address ip-prefix string
  + anycast-gw boolean
  - origin keyword
  + primary
  - status keyword
+ allow-directed-broadcast boolean
+ arp
  + debug keyword
  + duplicate-address-detection boolean
+ evpn
  + advertise route-type keyword
  + admin-tag number
+ host-route
  + populate route-type keyword
  + admin-tag number
+ learn-unsolicited boolean
+ neighbor ipv4-address string
  - datapath-programming
  - last-failed-complexes string
  - status keyword
  - expiration-time string
  + link-layer-address string
  - origin keyword
+ proxy-arp boolean
+ timeout number
+ virtual-ipv4-discovery
  + address ipv4-address string
  + allowed-macs string
  + probe-bridged-subinterfaces reference
  + probe-interval number
  - statistics
  - out-probe-packets number
  - statistics
  - out-total-probe-packets number
+ dhcp-client
  + trace-options
  + trace keyword
+ dhcp-relay
  + admin-state keyword
  + gi-address string
  + network-instance reference
  - oper-down-reason keyword
  - oper-state keyword
  + option keyword
  + server (ipv4-address | domain-name)
  - statistics
  - client-packets-discarded number
  - client-packets-received number
  - client-packets-relayed number
  - server-packets-discarded number
  - server-packets-received number
  - server-packets-relayed number
  + trace-options
  + trace keyword
+ use-gi-addr-as-src-ip-addr boolean

```

```

+ dhcp-server
+  admin-state keyword
-  oper-state keyword
-  statistics
-    in-discarded-packets number
-    in-error-packets number
-    in-forwarded-octets number
-    in-forwarded-packets number
-    in-matched-ra-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
+ ipv6
+  address ip-prefix string
+  anycast-gw boolean
-  origin keyword
+  primary
-  status keyword
+  dhcp-client
+  trace-options
+    trace keyword
+  dhcp-relay
+  admin-state keyword
+  network-instance reference
-  oper-down-reason keyword
-  oper-state keyword
+  option keyword
+  server (ipv6-address | domain-name)
+  source-address string
-  statistics
-    client-packets-discarded number
-    client-packets-received number
-    client-packets-relayed number
-    server-packets-discarded number
-    server-packets-received number
-    server-packets-relayed number
+  trace-options
+  trace keyword
+  dhcpv6-server
+  admin-state keyword
-  oper-state keyword
+  neighbor-discovery
+  debug keyword
+  duplicate-address-detection boolean
+  evpn
+  advertise route-type keyword
+  admin-tag number
+  host-route
+  populate route-type keyword
+  admin-tag number
+  learn-unsolicited keyword
+  neighbor ipv6-address string
-  current-state keyword
-  datapath-programming
-  last-failed-complexes string
-  status keyword

```

```

- is-router boolean
+ link-layer-address string
- next-state-time string
- origin keyword
+ proxy-nd boolean
+ reachable-time number
+ stale-time number
+ virtual-ipv6-discovery
+ address ipv6-address string
+ allowed-macs string
+ probe-bridged-subinterfaces reference
+ probe-interval number
- statistics
- out-probe-packets number
- statistics
- out-total-probe-packets number
+ router-advertisement
+ debug keyword
+ 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
- statistics
- in-discarded-packets number
- in-error-packets number
- in-forwarded-octets number
- in-forwarded-packets number
- in-matched-ra-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
+ l2-mtu number
- last-change string
+ local-mirror-destination
+ admin-state keyword
- oper-state keyword
- mpls
- statistics
- in-discarded-packets number
- in-error-packets number
- in-forwarded-octets number
- in-forwarded-packets number
- in-octets number
- in-packets number

```

```

- last-clear string
- 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
+ mpls-mtu number
- name string
- oper-down-reason keyword
- oper-state keyword
+ qos
+ input
+ classifiers
+ dot1p reference
+ dscp reference
+ ipv4-dscp reference
+ ipv6-dscp reference
+ mpls-traffic-class reference
+ policers
- policer index number
- committed-burst-size number
- committed-rate-kbps number
- maximum-burst-size number
- peak-rate-kbps number
- statistics
- accepted-octets number
- accepted-packets number
- committed-octets number
- committed-packets number
- dropped-octets number
- dropped-packets number
- exceeding-octets number
- exceeding-packets number
+ policer-template reference
+ output
+ rewrite-rules
+ dot1p reference
+ dscp reference
+ ipv4-dscp reference
+ ipv6-dscp reference
+ mpls-traffic-class reference
+ ra-guard
+ policy reference
+ vlan-list vlan-id number
- statistics
- in-discarded-packets number
- in-error-packets number
- in-forwarded-octets number
- in-forwarded-packets number
- in-matched-ra-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 | keyword)
+     untagged
+ tpid identityref
- traffic-rate
-   in-bps number
-   out-bps number
+ transceiver
-   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-down-reason keyword
- 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
+ tx-laser boolean
- 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

```

5.1 interface Descriptions

interface *name string*

Description	The list of named interfaces on the device.
Context	interface name string
Tree	interface
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	<p>The name of the interface</p> <p>Valid options are: irb<N>, N=0..255 lif-<lif_name> enp<bus>s<dev>f<fn>, bus=0..255, dev=0..31, fn=0..7 vhn-<vhn_name> lag<N>, N=1..128 [note1] lo<N>, N=0..255 mgmt0 mgmt0-standby ethernet-<slot>/<port> ethernet-<slot>/<mda>/<port> system0</p> <p><lif_name>=Linux interface name <vhn_name>=vhost interface name <slot>=slot number {1,2,3,..} <mda>=mda id {a,b,c,d} <port>=port id {1,2,3,..}</p> <p>[note1] N=1..32 for 7220-D1. N=1..48 for 7220-D2, 7220-D3. N=1..127 for 7220-H2, 7220-H3.</p>
Context	interface name string
String Length	3 to 132
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	The configured, desired state of the interface
Context	interface name string admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

breakout-mode

Description	Configuration of breakout options
Context	interface name <i>string</i> breakout-mode
Tree	breakout-mode
Configurable	True
Platforms	7220 IXR-D3L, 7220 IXR-D3

channel-speed *keyword*

Description	The speed of each channel (breakout port).
Context	interface name <i>string</i> breakout-mode channel-speed <i>keyword</i>
Tree	channel-speed
Options	<ul style="list-style-type: none"> • 10G • 25G
Configurable	True
Platforms	7220 IXR-D3L, 7220 IXR-D3

num-channels *keyword*

Description	The number of channels (breakout ports) supported by this connector.
Context	interface name <i>string</i> breakout-mode num-channels <i>keyword</i>
Tree	num-channels
Options	<ul style="list-style-type: none"> • 4
Configurable	True
Platforms	7220 IXR-D3L, 7220 IXR-D3

description *string*

Description	A user-configured description of the interface
Context	interface name <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

ethernet

Description	Enter the ethernet context
Context	interface name <i>string</i> ethernet
Tree	ethernet
Configurable	True
Platforms	Supported on all platforms

aggregate-id *reference*

Description	lag interface with which this interface is associated.
Context	interface name <i>string</i> ethernet aggregate-id <i>reference</i>
Tree	aggregate-id
Reference	interface name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

auto-negotiate *boolean*

Description	When set to true the interface uses auto-negotiation for speed, duplex and flow-control settings. When set to false, the transmission parameters are specified manually.
Context	interface name <i>string</i> ethernet auto-negotiate <i>boolean</i>
Tree	auto-negotiate
Configurable	True
Platforms	7220 IXR-D1

duplex-mode *keyword*

Description	When auto-negotiate is true, this sets the duplex mode that will be advertised to the peer. When auto-negotiate is false, this directly sets the duplex mode of the interface.
Context	interface name <i>string</i> ethernet duplex-mode <i>keyword</i>
Tree	duplex-mode
Options	<ul style="list-style-type: none"> • full • half

Configurable	True
Platforms	7220 IXR-D1

flow-control

Description	Enter the flow-control context
Context	interface name <i>string</i> ethernet flow-control
Tree	flow-control
Configurable	True
Platforms	Supported on all platforms

receive *boolean*

Description	<p>When this is true PAUSE frames received on this interface are accepted and processed, and, if auto-negotiation is enabled it also causes the capability to receive PAUSE frames to be signaled to the peer (applicable only to ports 1-48 of the 7220 IXR-D1 and to mgmt0 and mgmt0-standby ports).</p> <p>When this is false PAUSE frames received on this interface are ignored, and, if auto-negotiation is enabled it causes the capability to receive PAUSE frames to be signaled to the peer as non-support (applicable only to ports 1-48 of the 7220 IXR-D1 and to mgmt0 and mgmt0-standby ports)</p>
Context	interface name <i>string</i> ethernet flow-control receive <i>boolean</i>
Tree	receive
Configurable	True
Platforms	Supported on all platforms

hold-time

Description	Configure interface hold timers for Ethernet interfaces
Context	interface name <i>string</i> ethernet hold-time
Tree	hold-time
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

down *number*

Description	Holds link down events for the configured time.
--------------------	---

The hold-time down behavior is triggered with events that try to bring the ethernet interface down and can change quickly. It is not triggered with an admin-state disable event or interface disable due to other internal reasons (such as fabric unavailability). When running, the interface will not be brought down till the timer expires. The typical use of the hold-time down is to provide stability and avoid the protocols to advertise/withdraw messages if there are flapping optics. The hold-time down is aborted if the user does admin-state disable or if the interface is disabled due to other internal reasons that prevent the traffic to be forwarded on the interface.

Context	interface name <i>string</i> ethernet hold-time down <i>number</i>
Tree	down
Range	1 to 86400
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

down-expires *string*

Description	The remaining time until the hold-time down expires and the interface goes operationally down.
Context	interface name <i>string</i> ethernet hold-time down-expires <i>string</i>
Tree	down-expires
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

up *number*

Description	Holds link up events for the configured time. The hold-time up behavior is triggered with any event that tries to bring up the ethernet interface (interface admin-state enable, a reboot, etc). While the hold-time up is running, the transceiver laser will be enabled, however the higher layers will not be notified that the interface is operationally up until the timer expires.
Context	interface name <i>string</i> ethernet hold-time up <i>number</i>
Tree	up
Range	1 to 86400
Units	seconds
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

up-expires *string*

Description The remaining time until the hold-time up expires and the interface comes up.

Context [interface name](#) *string* [ethernet](#) [hold-time](#) [up-expires](#) *string*

Tree [up-expires](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

hw-mac-address *string*

Description The MAC address associated with the port

Context [interface name](#) *string* [ethernet](#) [hw-mac-address](#) *string*

Tree [hw-mac-address](#)

Configurable False

Platforms Supported on all platforms

l2cp-transparency

Description Configuration and state of the Layer-2 Control Protocol transparency

Context [interface name](#) *string* [ethernet](#) [l2cp-transparency](#)

Tree [l2cp-transparency](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dot1x

Description Container for the configuration of 802.1x Port based Network Access Control.

Context [interface name](#) *string* [ethernet](#) [l2cp-transparency](#) [dot1x](#)

Tree [dot1x](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-rule *keyword*

Description	The operational state of the TCAM rule applied to ingress dot1x frames.
Context	interface name <i>string</i> ethernet l2cp-transparency dot1x oper-rule <i>keyword</i>
Tree	oper-rule
Options	<ul style="list-style-type: none"> • trap-to-cpu-untagged • drop-tagged-and-untagged • tunnel-tagged-and-untagged
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tunnel *boolean*

Description	Configures if incoming dot1x frames are tunneled. Dot1x frames are identified by MAC DA 01-80-c2-00-00-03 and Ethertype 0x888e.
Context	interface name <i>string</i> ethernet l2cp-transparency dot1x tunnel <i>boolean</i>
Tree	tunnel
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lACP

Description	Container for L2CP transparency of the Link Aggregation Control Protocol
Context	interface name <i>string</i> ethernet l2cp-transparency lACP
Tree	lACP
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-rule *keyword*

Description	The operational state of the TCAM rule applied to ingress LACP frames.
Context	interface name <i>string</i> ethernet l2cp-transparency lACP oper-rule <i>keyword</i>
Tree	oper-rule
Options	<ul style="list-style-type: none"> • trap-to-cpu-untagged

	<ul style="list-style-type: none"> • drop-tagged-and-untagged • tunnel-tagged-and-untagged
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tunnel *boolean*

Description	Configures if incoming LACP frames are tunneled. LACP frames are identified by MAC DA 01-80-c2-00-00-02, Ethertype 0x8809 and slow-protocol sub-type 0x01.
Context	interface name <i>string</i> ethernet l2cp-transparency lacp tunnel <i>boolean</i>
Tree	tunnel
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lldp

Description	Container for L2CP transparency of the Link Layer Discovery Protocol
Context	interface name <i>string</i> ethernet l2cp-transparency lldp
Tree	lldp
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-rule *keyword*

Description	The operational state of the TCAM rule applied to ingress LLDP frames.
Context	interface name <i>string</i> ethernet l2cp-transparency lldp oper-rule <i>keyword</i>
Tree	oper-rule
Options	<ul style="list-style-type: none"> • trap-to-cpu-untagged • drop-tagged-and-untagged • tunnel-tagged-and-untagged
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tunnel *boolean*

Description	Configures if incoming LLDP frames are tunneled. LLDP frames are identified by MAC DA 01-80-c2-00-00-00 and Ethertype 0x88cc.
Context	interface name <i>string</i> ethernet l2cp-transparency lldp tunnel <i>boolean</i>
Tree	tunnel
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ptp

Description	Container for the configuration of Precision Time Protocol Peer-Delay frames.
Context	interface name <i>string</i> ethernet l2cp-transparency ptp
Tree	ptp
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-rule *keyword*

Description	The operational state of the TCAM rule applied to ingress ptp frames.
Context	interface name <i>string</i> ethernet l2cp-transparency ptp oper-rule <i>keyword</i>
Tree	oper-rule
Options	<ul style="list-style-type: none"> • trap-to-cpu-untagged • drop-tagged-and-untagged • tunnel-tagged-and-untagged
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tunnel *boolean*

Description	Configures if incoming ptp frames are tunneled. ptp frames are identified by MAC DA 01-80-c2-00-00-0e and Ethertype 0x88f7.
Context	interface name <i>string</i> ethernet l2cp-transparency ptp tunnel <i>boolean</i>

Tree	tunnel
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tunnel-all-l2cp *boolean*

Description	Configures the tunneling of all the L2CP protocols. When set to true this command triggers the installation of an ingress TCAM rule with the highest priority (above all the individual L2CP tunnel rules) which allows the forwarding of any Layer-2 Control Protocol coming into the interface. All the L2CP frames identified by MAC DA = 01:80:c2:00:00:0x or MAC DA = 01:80:c2:00:00:2x, with 'x' being any hex value, are tunneled. When set to false, all L2CP frames without a specific L2CP tunnel rule are discarded.
Context	interface name <i>string</i> ethernet l2cp-transparency tunnel-all-l2cp <i>boolean</i>
Tree	tunnel-all-l2cp
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

xstp

Description	Container for the configuration of all the Spanning Tree Protocols. It includes Spanning Tree Protocol (STP), Rapid RSTP (RSTP) and Multiple STP (MSTP)
Context	interface name <i>string</i> ethernet l2cp-transparency xstp
Tree	xstp
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-rule *keyword*

Description	The operational state of the TCAM rule applied to ingress xSTP frames.
Context	interface name <i>string</i> ethernet l2cp-transparency xstp oper-rule <i>keyword</i>
Tree	oper-rule
Options	<ul style="list-style-type: none"> • trap-to-cpu-untagged • drop-tagged-and-untagged

	<ul style="list-style-type: none"> tunnel-tagged-and-untagged
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tunnel *boolean*

Description	Configures if incoming xSTP frames are tunneled. xSTP frames are identified by MAC DA 01-80-c2-00-00-00 and any Ethertype.
Context	interface name <i>string</i> ethernet l2cp-transparency xstp tunnel <i>boolean</i>
Tree	tunnel
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lACP-port-priority *number*

Description	Configure the port priority for LACP. This value is used to determine which port should be activated with LACP fallback mode. Lower values are more preferred.
Context	interface name <i>string</i> ethernet lACP-port-priority <i>number</i>
Tree	lACP-port-priority
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

physical-medium *keyword*

Description	Indicates the PHY supported by the RJ45 port. If the port is supported by a SFP, QSFP+, QSFP28 or QSFP-DD transceiver no value is populated in this leaf.
Context	interface name <i>string</i> ethernet physical-medium <i>keyword</i>
Tree	physical-medium
Options	<ul style="list-style-type: none"> 1000BASE-T
Configurable	False
Platforms	Supported on all platforms

port-speed *keyword***Description**

The speed of the port or channel

The default speed of a port (when there is no configured value and auto-negotiation is disabled or unsupported) depends on the platform and port/connector number as follows:

mgmt0 and mgmt0-standby ports: 1G J2 IMM ports 1-32: 100G J2 IMM ports 33-36: 100G 7220-D1 ports 1-48: 1G 7220-D1 ports 49-52: 10G 7220-D2/D2L ports 1-48: 25G 7220-D2/D2L ports 49-56: 100G 7220-D2L ports 57-58: 10G 7220-D3 ports 1-2: 10G 7220-D3 ethernet-1/[3-34]: 100G 7220-D3 ethernet-1/[3-33]/n: 25G 7220-D3L ethernet-1/[1-32]: 100G 7220-D3L ethernet-1/[1-31]/n: 25G 7220-D3L ports 33-34: 10G 7220-D5 ports 1-32: 400G 7220-D5 ports 33-38: 10G 7220-H2 ports 1-128: 100G 7220-H3 ports 1-2: 10G 7220-H3 ports 3-34: 400G

Supported speeds: mgmt0 and mgmt0-standby ports: 1G J2 IMM ports 1-32: 40G, 100G [note1] J2 IMM ports 33-36: 40G, 100G, 400G 7220-D1 ports 1-48: 10M, 100M, 1G 7220-D1 ports 49-52: 10G 7220-D2/D2L ports 1-48: 1G, 10G, 25G [note2] 7220-D2/D2L ports 49-56: 40G, 100G 7220-D2L ports 57-58: 10G 7220-D3 ports 1-2: 10G 7220-D3 ethernet-1/[3-34]: 40G, 100G 7220-D3 ethernet-1/[3-33]/n: 10G, 25G 7220-D3L ethernet-1/[1-32]: 40G, 100G 7220-D3L ethernet-1/[1-31]/n: 10G, 25G 7220-D3L ports 33-34: 10G 7220-D5 ports 1-32: 40G, 100G, 400G 7220-D5 ports 33-38: 10G 7220-H2 ports 1-128: 100G 7220-H3 ports 1-2: 10G 7220-H3 ports 3-34: 40G, 100G, 400G

[note1] Ports 9-12 cannot operate at different port speeds (some at 40G and others at 100G). The required speed of ports 9-12 is based on the port-speed of the lowest-numbered configured port in this block; if any higher-numbered port in the block is configured with a different port speed that port will not come up.

[note2] On 7220-D2: if one port in each consecutive group of 4 ports (1-4, 5-8, .. , 45-48) is 25G the other 3 ports must also be 25G; if one port in each consecutive group of 4 ports (1-4, 5-8, .. , 45-48) is 1G or 10G the other 3 ports must also be 1G or 10G. On 7220-D2L: if one port in each consecutive group of 12 ports (1-12, 13-24, 25-36, 37-48) is 25G the other 11 ports must also be 25G; if one port in each consecutive group of 12 ports (1-12, 13-24, 25-36, 37-48) is 1G or 10G the other 11 ports must also be 1G or 10G.

7250 IXR details: If the interface corresponds to a connector that has no installed transceiver then the value is accepted without any checking or restriction, and info from state will display the configured value. Otherwise if the configured port-speed is NOT supported by the installed transceiver the port is forced operationally down.

Context

[interface name](#) *string* [ethernet port-speed](#) *keyword*

Tree

[port-speed](#)

Options

- 10M
- 100M
- 1G
- 10G

	<ul style="list-style-type: none"> • 25G • 40G • 50G • 100G • 200G • 400G • 1T
Configurable	True
Platforms	Supported on all platforms

reload-delay *number*

Description	<p>Configure reload-delay timer for Ethernet interfaces.</p> <p>The reload-delay timer starts when the associated XDP interface state is learned. While the timer is running, the interface transceiver laser is disabled to avoid attracting traffic from the connected device at the other end of the interface. The reload-delay timer should be used in multi-homing interfaces and be set to a value long enough to allow the system to recover all the network protocols upon reboot, before start attracting traffic from the multi-homed device.</p>
Context	interface name <i>string</i> ethernet reload-delay <i>number</i>
Tree	reload-delay
Range	1 to 86400
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

reload-delay-expires *string*

Description	The remaining time until the reload-delay expires and the interface can go operationally up.
Context	interface name <i>string</i> ethernet reload-delay-expires <i>string</i>
Tree	reload-delay-expires
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

standby-signaling *keyword*

Description	Indicates the standby-signaling used in the interface. An application using a port-based redundancy mechanism will trigger the standby signaling on the ethernet interface if the interface is selected as standby.
Context	interface name <i>string</i> ethernet standby-signaling <i>keyword</i>
Tree	standby-signaling
Options	<ul style="list-style-type: none"> power-off lacp
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> ethernet statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

in-1024b-to-1518b-frames *number*

Description	Number of received Ethernet frames that are 1024-1518 bytes in length
Context	interface name <i>string</i> ethernet statistics in-1024b-to-1518b-frames <i>number</i>
Tree	in-1024b-to-1518b-frames
Default	0
Configurable	False
Platforms	Supported on all platforms

in-128b-to-255b-frames *number*

Description	Number of received Ethernet frames that are 128-255 bytes in length
Context	interface name <i>string</i> ethernet statistics in-128b-to-255b-frames <i>number</i>
Tree	in-128b-to-255b-frames
Default	0
Configurable	False

Platforms Supported on all platforms

in-1519b-or-longer-frames *number*

Description Number of received Ethernet frames that are 1519 bytes or longer

Context [interface name](#) *string* [ethernet statistics in-1519b-or-longer-frames](#) *number*

Tree [in-1519b-or-longer-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-256b-to-511b-frames *number*

Description Number of received Ethernet frames that are 256-511 bytes in length

Context [interface name](#) *string* [ethernet statistics in-256b-to-511b-frames](#) *number*

Tree [in-256b-to-511b-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-512b-to-1023b-frames *number*

Description Number of received Ethernet frames that are 512-1023 bytes in length

Context [interface name](#) *string* [ethernet statistics in-512b-to-1023b-frames](#) *number*

Tree [in-512b-to-1023b-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-64b-frames *number*

Description Number of received Ethernet frames that are exactly 64 bytes in length

Context [interface name](#) *string* [ethernet statistics in-64b-frames](#) *number*

Tree [in-64b-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-65b-to-127b-frames *number*

Description Number of received Ethernet frames that are 65-127 bytes in length

Context [interface name](#) *string* [ethernet statistics in-65b-to-127b-frames](#) *number*

Tree [in-65b-to-127b-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-crc-error-frames *number*

Description Number of receive error events due to FCS/CRC check failure.

Context [interface name](#) *string* [ethernet statistics in-crc-error-frames](#) *number*

Tree [in-crc-error-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-fragment-frames *number*

Description Number of fragment frames received on the interface.

Context [interface name](#) *string* [ethernet statistics in-fragment-frames](#) *number*

Tree [in-fragment-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-jabber-frames *number*

Description Number of jabber frames received on the interface. Jabber frames are typically defined as oversize frames which also have a bad CRC.

Context [interface name](#) *string* [ethernet statistics in-jabber-frames](#) *number*

Tree [in-jabber-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-mac-pause-frames *number*

Description Number of MAC layer PAUSE frames received on the interface.

Context [interface name](#) *string* [ethernet statistics in-mac-pause-frames](#) *number*

Tree [in-mac-pause-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

in-oversize-frames *number*

Description Number of oversize frames received on the interface (i.e. frames that exceed the operational port MTU)

Context [interface name](#) *string* [ethernet statistics in-oversize-frames](#) *number*

Tree [in-oversize-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

last-clear *string*

Description Timestamp of the last time the MAC counters were cleared.

Context [interface name](#) *string* [ethernet statistics last-clear](#) *string*

Tree [last-clear](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

out-1024b-to-1518b-frames *number*

Description Number of transmitted Ethernet frames that are 1024-1518 bytes in length

Context [interface name](#) *string* [ethernet statistics out-1024b-to-1518b-frames](#) *number*

Tree [out-1024b-to-1518b-frames](#)

Default 0

Configurable False

Platforms Supported on all platforms

out-128b-to-255b-frames *number*

Description Number of transmitted Ethernet frames that are 128-255 bytes in length
Context [interface name](#) *string* [ethernet statistics out-128b-to-255b-frames](#) *number*
Tree [out-128b-to-255b-frames](#)
Default 0
Configurable False
Platforms Supported on all platforms

out-1519b-or-longer-frames *number*

Description Number of transmitted Ethernet frames that are 1519 bytes or longer
Context [interface name](#) *string* [ethernet statistics out-1519b-or-longer-frames](#) *number*
Tree [out-1519b-or-longer-frames](#)
Default 0
Configurable False
Platforms Supported on all platforms

out-256b-to-511b-frames *number*

Description Number of transmitted Ethernet frames that are 256-511 bytes in length
Context [interface name](#) *string* [ethernet statistics out-256b-to-511b-frames](#) *number*
Tree [out-256b-to-511b-frames](#)
Default 0
Configurable False
Platforms Supported on all platforms

out-512b-to-1023b-frames *number*

Description Number of transmitted Ethernet frames that are 512-1023 bytes in length
Context [interface name](#) *string* [ethernet statistics out-512b-to-1023b-frames](#) *number*
Tree [out-512b-to-1023b-frames](#)
Default 0
Configurable False

Platforms Supported on all platforms

out-64b-frames *number*

Description Number of transmitted Ethernet frames that are exactly 64 bytes in length
Context [interface name](#) *string* [ethernet statistics out-64b-frames](#) *number*
Tree [out-64b-frames](#)
Default 0
Configurable False
Platforms Supported on all platforms

out-65b-to-127b-frames *number*

Description Number of transmitted Ethernet frames that are 65-127 bytes in length
Context [interface name](#) *string* [ethernet statistics out-65b-to-127b-frames](#) *number*
Tree [out-65b-to-127b-frames](#)
Default 0
Configurable False
Platforms Supported on all platforms

out-mac-pause-frames *number*

Description Number of MAC layer PAUSE frames sent on the interface.
Context [interface name](#) *string* [ethernet statistics out-mac-pause-frames](#) *number*
Tree [out-mac-pause-frames](#)
Default 0
Configurable False
Platforms Supported on all platforms

storm-control

Description Enable the storm-control context
Context [interface name](#) *string* [ethernet storm-control](#)
Tree [storm-control](#)
Configurable True
Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

broadcast-rate *number*

Description	The maximum rate allowed for ingress broadcast frames on the interface
Context	interface name <i>string</i> ethernet storm-control broadcast-rate <i>number</i>
Tree	broadcast-rate
Range	0 to 100000000
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

multicast-rate *number*

Description	The maximum rate allowed for ingress multicast frames on the interface
Context	interface name <i>string</i> ethernet storm-control multicast-rate <i>number</i>
Tree	multicast-rate
Range	0 to 100000000
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

operational-broadcast-rate *number*

Description	The operational maximum rate for ingress broadcast frames programmed on the interface
Context	interface name <i>string</i> ethernet storm-control operational-broadcast-rate <i>number</i>
Tree	operational-broadcast-rate
Units	kbps
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

operational-multicast-rate *number*

Description	The operational maximum rate for ingress multicast frames programmed on the interface
Context	interface name <i>string</i> ethernet storm-control operational-multicast-rate <i>number</i>
Tree	operational-multicast-rate
Units	kbps

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

operational-unknown-unicast-rate *number*

Description	The operational maximum rate for ingress unknown unicast frames programmed on the interface
Context	interface name <i>string</i> ethernet storm-control operational-unknown-unicast-rate <i>number</i>
Tree	operational-unknown-unicast-rate
Units	kbps
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

units *keyword*

Description	Units of storm-control policer in kbps or percentage of the interface bandwidth
Context	interface name <i>string</i> ethernet storm-control units <i>keyword</i>
Tree	units
Default	percentage
Options	<ul style="list-style-type: none"> • kbps • percentage
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

unknown-unicast-rate *number*

Description	The maximum rate allowed for ingress unknown unicast frames on the interface
Context	interface name <i>string</i> ethernet storm-control unknown-unicast-rate <i>number</i>
Tree	unknown-unicast-rate
Range	0 to 100000000
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ifindex number

Description	System-wide persistent unique ifIndex assigned to the interface
Context	interface name <i>string</i> ifindex number
Tree	ifindex
Configurable	False
Platforms	Supported on all platforms

lag

Description	Container for options related to LAG
Context	interface name <i>string</i> lag
Tree	lag
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp

Description	LACP parameters for the associated LAG
Context	interface name <i>string</i> lag lacp
Tree	lacp
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-key number

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.
Context	interface name <i>string</i> lag lacp admin-key number
Tree	admin-key
Range	1 to 65535
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interval *keyword*

Description	Set the period between LACP messages -- uses the lacp-period-type enumeration.
Context	interface name <i>string</i> lag lacp interval <i>keyword</i>
Tree	interval
Default	SLOW
Options	<ul style="list-style-type: none"> FAST Send LACP packets every second SLOW Send LACP packets every 30 seconds
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp-mode *keyword*

Description	ACTIVE is to initiate the transmission of LACP packets. PASSIVE is to wait for peer to initiate the transmission of LACP packets.
Context	interface name <i>string</i> lag lacp lacp-mode <i>keyword</i>
Tree	lacp-mode
Default	ACTIVE
Options	<ul style="list-style-type: none"> 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
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

system-id-mac *string*

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.
Context	interface name <i>string</i> lag lacp system-id-mac <i>string</i>
Tree	system-id-mac
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

system-priority *number*

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.

Context [interface name](#) *string lag lacp system-priority number*

Tree [system-priority](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp-fallback-mode *keyword*

Description Specifies lacp-fallback mode if enabled

Context [interface name](#) *string lag lacp-fallback-mode keyword*

Tree [lacp-fallback-mode](#)

Options

- static
Set the LACP-fallback mode as static

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp-fallback-timeout *number*

Description Specifies the LACP-fallback timeout interval in seconds

Context [interface name](#) *string lag lacp-fallback-timeout number*

Tree [lacp-fallback-timeout](#)

Range 4 to 3600

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lag-speed *number*

Description Reports current aggregate bandwidth speed of the associated LAG

Context	interface name <i>string lag lag-speed number</i>
Tree	lag-speed
Units	Mbps
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lag-type *keyword*

Description	Sets the type of LAG, i.e., how it is configured / maintained
Context	interface name <i>string lag lag-type keyword</i>
Tree	lag-type
Default	static
Options	<ul style="list-style-type: none"> • <code>lacp</code> LAG managed by LACP • <code>static</code> Statically configured bundle / LAG
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

member [name](#) *reference*

Description	Reports the list of interfaces associated with the LAG instance
Context	interface name <i>string lag member name reference</i>
Tree	member
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *reference*

Description	Enter the name context
Context	interface name <i>string lag member name reference</i>
Reference	interface name <i>string</i>
Configurable	False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp

Description Operational status data for the member interfaces

Context [interface name](#) *string* [lag member name](#) *reference* [lacp](#)

Tree [lacp](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

activity *keyword*

Description Indicates participant is active or passive

Context [interface name](#) *string* [lag member name](#) *reference* [lacp activity keyword](#)

Tree [activity](#)

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

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

aggregatable *boolean*

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

Context [interface name](#) *string* [lag member name](#) *reference* [lacp aggregatable boolean](#)

Tree [aggregatable](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

collecting *boolean*

Description	If true, the participant is collecting incoming frames on the link, otherwise false
Context	interface name <i>string</i> lag member name <i>reference</i> lACP collecting <i>boolean</i>
Tree	collecting
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

distributing *boolean*

Description	When true, the participant is distributing outgoing frames; when false, distribution is disabled
Context	interface name <i>string</i> lag member name <i>reference</i> lACP distributing <i>boolean</i>
Tree	distributing
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lACP-port-priority *number*

Description	Configures the port priority for LACP. This value is used to determine which port should be activated with LACP fallback mode. Lower values are more preferred.
Context	interface name <i>string</i> lag member name <i>reference</i> lACP lACP-port-priority <i>number</i>
Tree	lACP-port-priority
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-key *number*

Description	Current operational value of the key for the aggregate interface
Context	interface name <i>string</i> lag member name <i>reference</i> lACP oper-key <i>number</i>
Tree	oper-key
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

partner-id *string*

Description	MAC address representing the protocol partner's interface system ID
Context	interface name <i>string</i> lag member name <i>reference</i> lACP partner-id <i>string</i>
Tree	partner-id
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

partner-key *number*

Description	Operational value of the protocol partner's key
Context	interface name <i>string</i> lag member name <i>reference</i> lACP partner-key <i>number</i>
Tree	partner-key
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

partner-port-num *number*

Description	Port number of the partner (remote) port for this member port
Context	interface name <i>string</i> lag member name <i>reference</i> lACP partner-port-num <i>number</i>
Tree	partner-port-num
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

port-num *number*

Description	Port number of the local (actor) aggregation member
Context	interface name <i>string</i> lag member name <i>reference</i> lACP port-num <i>number</i>
Tree	port-num
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

statistics

Description	LACP protocol counters
Context	interface name <i>string</i> lag member name <i>reference</i> lACP statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lACP-errors *number*

Description	Number of LACPDU illegal packet errors
Context	interface name <i>string</i> lag member name <i>reference</i> lACP statistics lACP-errors <i>number</i>
Tree	lACP-errors
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lACP-in-pkts *number*

Description	Number of LACPDU received
Context	interface name <i>string</i> lag member name <i>reference</i> lACP statistics lACP-in-pkts <i>number</i>
Tree	lACP-in-pkts
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lACP-out-pkts *number*

Description	Number of LACPDU transmitted
Context	interface name <i>string</i> lag member name <i>reference</i> lACP statistics lACP-out-pkts <i>number</i>
Tree	lACP-out-pkts
Default	0
Configurable	False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp-rx-errors *number*

Description Number of LACPDU receive packet errors

Context [interface name](#) *string* [lag member name](#) *reference* [lacp statistics lacp-rx-errors](#) *number*

Tree [lacp-rx-errors](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp-tx-errors *number*

Description Number of LACPDU transmit packet errors

Context [interface name](#) *string* [lag member name](#) *reference* [lacp statistics lacp-tx-errors](#) *number*

Tree [lacp-tx-errors](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lacp-unknown-errors *number*

Description Number of LACPDU unknown packet errors

Context [interface name](#) *string* [lag member name](#) *reference* [lacp statistics lacp-unknown-errors](#) *number*

Tree [lacp-unknown-errors](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

synchronization *keyword*

Description Indicates whether the participant is in-sync or out-of-sync

Context	interface name <i>string</i> lag member name <i>reference</i> lACP synchronization <i>keyword</i>
Tree	synchronization
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
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

system-id *string*

Description	MAC address that defines the local system ID for the aggregate interface
Context	interface name <i>string</i> lag member name <i>reference</i> lACP system-id <i>string</i>
Tree	system-id
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

timeout *keyword*

Description	The timeout type (short or long) used by the participant
Context	interface name <i>string</i> lag member name <i>reference</i> lACP timeout <i>keyword</i>
Tree	timeout
Options	<ul style="list-style-type: none"> • 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
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-change *string*

Description	The date and time of the most recent change to the LAG member-link state
Context	interface name <i>string</i> lag member name <i>reference</i> last-change <i>string</i>
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

microbfd-enabled *boolean*

Description	Indicates if microBFD is currently used in the determination of the member-link oper-status
Context	interface name <i>string</i> lag member name <i>reference</i> microbfd-enabled <i>boolean</i>
Tree	microbfd-enabled
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-down-reason *keyword*

Description	Reason for operational down state for the associated LAG
Context	interface name <i>string</i> lag member name <i>reference</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • port-disabled • port-oper-disabled • lag-admin-disabled • lacp-down • microBFD-down • lag-min-link-threshold • lag-speed-mismatch • other
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-state *keyword*

Description	Operational state for the associated LAG
Context	interface name <i>string</i> lag member name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the <code>reinvoke-with-delay</code> action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

member-speed *keyword*

Description	Specifies the link speed of allowed member-links
Context	interface name <i>string lag member-speed keyword</i>
Tree	member-speed
Options	<ul style="list-style-type: none"> • 10M Indicates the the LAG member-links must be 10M to be active • 100M Indicates the the LAG member-links must be 100M to be active • 1G Indicates the the LAG member-links must be 1G to be active • 10G Indicates the the LAG member-links must be 10G to be active • 25G Indicates the the LAG member-links must be 25G to be active • 40G Indicates the the LAG member-links must be 40G to be active • 100G Indicates the the LAG member-links must be 100G to be active • 400G Indicates the the LAG member-links must be 400G to be active

Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

min-links *number*

Description	Specifies the minimum number of member interfaces that must be active for the aggregate interface to be available
Context	interface name <i>string lag min-links number</i>
Tree	min-links
Range	1 to 64
Default	1

Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-change *string*

Description	The date and time of the most recent change to the interface state
Context	interface name <i>string</i> last-change <i>string</i>
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

loopback-mode *boolean*

Description	When loopback-mode is set to true the port loops back packets that come in via the port
Context	interface name <i>string</i> loopback-mode <i>boolean</i>
Tree	loopback-mode
Configurable	True
Platforms	Supported on all platforms

mtu *number*

Description	<p>Port MTU in bytes including ethernet overhead but excluding 4-bytes FCS. If a transmitted packet exceeds this size it is dropped.</p> <p>The default value for ethernet-x interfaces is taken from /system/mtu/default-port-mtu. For the mgmt0 and mgmt0-standby interfaces the default is 1514 bytes, but the value can be changed for each interface individually. Port MTU is not configurable for loopback interfaces.</p> <p>The 7220 IXR-D1, 7220 IXR-D2, 7220 IXR-D3, 7220 IXR-H2, and 7220 IXR-H3 systems support a maximum port MTU of 9412 bytes.</p> <p>Each 7250 IXR IMM supports a maximum of 8 different port MTU values. 7220 IXR systems do not have any limit on the maximum number of different port MTU values.</p>
Context	interface name <i>string</i> mtu <i>number</i>
Tree	mtu
Range	1500 to 9500

Units	bytes
Configurable	True
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The first (and possibly only) reason for the port being operationally down
Context	interface name <i>string</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • port-admin-disabled • mda-admin-disabled • transceiver-oper-down • loopback • port-not-present • mda-not-present • phy-initializing • lower-layer-down • auto-negotiation-mismatch • port-mtu-resource-exceeded • unsupported-speed • unsupported-fec • other • fabric-availability • no-active-links • min-link-threshold • port-9-12-speed-mismatch • lag-resource-exceeded • lag-member-resource-exceeded • standby-signaling • interface-hold-time-up-active • interface-reload-timer-active • connector-down • event-handler
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of the interface
Context	interface name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up • down
Configurable	False
Platforms	Supported on all platforms

qos

Description	Enable the qos context
Context	interface name <i>string</i> qos
Tree	qos
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

output

Description	Container for QoS configuration that applies to outbound traffic through the port or LAG
Context	interface name <i>string</i> qos output
Tree	output
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

multicast-queue [queue-id](#) *number*

Description	List of multicast queues
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i>
Tree	multicast-queue
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

queue-id *number*

Description	The queue identifier For J2 and TD3 there is a one-to-one mapping between queue-id and forwarding class. fc0 traffic always use queue-id 0, fc1 traffic always uses queue-id 1, etc. For TH3 the multicast queue-id range is limited to 0-3 and the mapping is as follows: fc0+1 -> queue-id 0 fc2+3 -> queue-id 1 fc4+5 -> queue-id 2 fc6+7 -> queue-id 3
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i>
Range	0 to 7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

forwarding-class *keyword*

Description	The list of forwarding classes that map to this queue.
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> forwarding-class <i>keyword</i>
Tree	forwarding-class
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

queue-depth

Description	Enter the queue-depth context
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> queue-depth
Tree	queue-depth
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

last-high-threshold-time *string*

Description	The last time the queue depth exceeded the high-threshold in a rising direction.
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> queue-depth last-high-threshold-time <i>string</i>
Tree	last-high-threshold-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

maximum-burst-size *number*

Description	Maximum queue depth in bytes.
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> queue-depth maximum-burst-size <i>number</i>
Tree	maximum-burst-size
Units	bytes
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

scheduling

Description	Container for queue scheduling parameters
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> scheduling
Tree	scheduling
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

peak-rate-bps *number*

Description	The actual/operational peak rate in bits per second.
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> scheduling peak-rate-bps <i>number</i>
Tree	peak-rate-bps
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

peak-rate-percent *number*

Description	The maximum percentage of port bandwidth that is available to the traffic in this multicast queue. The default is 100.
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> scheduling peak-rate-percent <i>number</i>
Tree	peak-rate-percent
Range	1 to 100
Default	100
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

scheduler-node *reference*

Description	The scheduler node to which the multicast queue is connected. The mappings are fixed and not user-configurable. J2: queue-id 0-7 -> node 0 TD3 (D2/D3): queue-id 0 -> node 0 queue-id 1 -> node 1 queue-id 2 -> node 2 queue-id 3 -> node 3 queue-id 4 -> node 4 queue-id 5 -> node 5 queue-id 6 -> node 6 queue-id 7 -> node 7 TH3: queue-id 4 -> node 0 queue-id 5 -> node 3 queue-id 6 -> node 6 queue-id 7 -> node 9
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> scheduling scheduler-node <i>reference</i>
Tree	scheduler-node
Reference	interface name <i>string</i> qos output scheduler tier level <i>number</i> node node-number <i>number</i>
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

template *reference*

Description	The name of a queue-template to apply to the multicast queue. The active-queue-management container must not be present in order to apply the template. Also the high-threshold-bytes configuration in this template is ignored.
Context	interface name <i>string</i> qos output multicast-queue queue-id <i>number</i> template <i>reference</i>
Tree	template

Reference	qos queue-templates queue-template name string
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

scheduler

Description	Output traffic scheduler options
Context	interface name string qos output scheduler
Tree	scheduler
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

tier level number

Description	List of output traffic scheduler tiers or levels
Context	interface name string qos output scheduler tier level number
Tree	tier
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1
Max. Elements	1

level number

Description	Enter the level context
Context	interface name string qos output scheduler tier level number
Range	1 to 4
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

node node-number number

Description	List of scheduler nodes at the specified scheduler level
Context	interface name string qos output scheduler tier level number node node-number number
Tree	node
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

Max. Elements 12

node-number *number*

Description An identifier of the scheduler node. Within a scheduler tier, higher-numbered nodes are served before lower-numbered nodes.

Context [interface name](#) *string* [qos output scheduler tier level](#) *number* [node node-number](#) *number*

Range 0 to 11

Configurable True

Platforms Supported on all platforms except 7220 IXR-D1

strict-priority *boolean*

Description A true value configures the node for strict priority scheduling, whether or not a weight is also configured. When set to false the node is serviced using DWRR, even if the node does not have a configured weight; in this case the default weight value of 1 is used.

Context [interface name](#) *string* [qos output scheduler tier level](#) *number* [node node-number](#) *number* [strict-priority](#) *boolean*

Tree [strict-priority](#)

Configurable True

Platforms Supported on all platforms except 7220 IXR-D1

weight *number*

Description The DWRR weight assigned to the scheduler node

Context [interface name](#) *string* [qos output scheduler tier level](#) *number* [node node-number](#) *number* [weight](#) *number*

Tree [weight](#)

Range 1 to 127

Default 1

Configurable True

Platforms Supported on all platforms except 7220 IXR-D1

unicast-queue [queue-id](#) *number*

Description List of unicast queues

Context [interface name](#) *string* [qos output unicast-queue](#) [queue-id](#) *number*

Tree	unicast-queue
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

queue-id *number*

Description	The queue identifier For unicast traffic on all platforms there is a one-to-one mapping between queue-id and forwarding class. fc0 traffic always use queue-id 0, fc1 traffic always uses queue-id 1, etc.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i>
Range	0 to 7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

active-queue-management

Description	Enter the active-queue-management context
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management
Tree	active-queue-management
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

ecn-slope [ecn-drop-probability](#) *keyword*

Description	List of ECN slopes.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i>
Tree	ecn-slope
Configurable	False
Platforms	Supported on all platforms

ecn-drop-probability *keyword*

Description	The drop probability to which the ECN slope applies.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i>

Options	<ul style="list-style-type: none"> low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red. all All traffic, consisting of traffic marked low, medium and high drop-probability.
Configurable	False
Platforms	Supported on all platforms

max-probability *number*

Description	<p>The maximum probability of marking a packet (at or above the max-threshold).</p> <p>On 7250 IXR systems there can be a significant difference between the configured value and the operational value.</p>
Context	interface name <i>string</i> qos output unicast-queue queue-id number active-queue-management ecn-slope ecn-drop-probability <i>keyword</i> max-probability number
Tree	max-probability
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

max-threshold-bytes *number*

Description	The queue depth in bytes that corresponds to the ECN maximum threshold parameter.
Context	interface name <i>string</i> qos output unicast-queue queue-id number active-queue-management ecn-slope ecn-drop-probability <i>keyword</i> max-threshold-bytes number
Tree	max-threshold-bytes
Units	bytes
Configurable	False

Platforms Supported on all platforms

min-threshold-bytes *number*

Description The queue depth in bytes that corresponds to the ECN minimum threshold parameter.

Context [interface name](#) *string* [qos output unicast-queue queue-id](#) *number* [active-queue-management ecn-slope ecn-drop-probability](#) *keyword* [min-threshold-bytes](#) *number*

Tree [min-threshold-bytes](#)

Units bytes

Configurable False

Platforms Supported on all platforms

slope-enabled *boolean*

Description Reads true if the slope is enabled.
A disabled slope has min-threshold-bytes = max-threshold-bytes = max-probability = 0

Context [interface name](#) *string* [qos output unicast-queue queue-id](#) *number* [active-queue-management ecn-slope ecn-drop-probability](#) *keyword* [slope-enabled](#) *boolean*

Tree [slope-enabled](#)

Configurable False

Platforms Supported on all platforms

wred-slope [traffic-type](#) *keyword* [drop-probability](#) *keyword*

Description List of WRED slopes.

Context [interface name](#) *string* [qos output unicast-queue queue-id](#) *number* [active-queue-management wred-slope traffic-type](#) *keyword* [drop-probability](#) *keyword*

Tree [wred-slope](#)

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

traffic-type *keyword*

Description The traffic type to which the WRED slope applies.

Context	<code>interface name string qos output unicast-queue queue-id number active-queue-management wred-slope traffic-type keyword drop-probability keyword</code>
Options	<ul style="list-style-type: none"> • tcp Refers to IPv4/IPv6 packets with a protocol/next-header indicating a value of 6. • non-tcp Refers to all packets that are not IPv4/IPv6 packets with a protocol/next-header indicating a value of 6. • all Refers to all traffic, whether it is TCP or non-TCP.
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability *keyword*

Description	The drop probability to which the WRED slope applies.
Context	<code>interface name string qos output unicast-queue queue-id number active-queue-management wred-slope traffic-type keyword drop-probability keyword</code>
Options	<ul style="list-style-type: none"> • low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. • medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. • high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

max-probability *number*

Description	<p>The maximum probability of dropping a packet (at or above the max-threshold).</p> <p>On 7250 IXR systems there can be a significant difference between the configured value and the operational value.</p>
--------------------	---

Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> max-probability <i>number</i>
Tree	max-probability
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

max-threshold-bytes *number*

Description	The queue depth in bytes that corresponds to the WRED maximum threshold parameter.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> max-threshold-bytes <i>number</i>
Tree	max-threshold-bytes
Units	bytes
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

min-threshold-bytes *number*

Description	The queue depth in bytes that corresponds to the WRED minimum threshold parameter.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> min-threshold-bytes <i>number</i>
Tree	min-threshold-bytes
Units	bytes
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

slope-enabled *boolean*

Description	Reads true if the slope is enabled. A disabled slope has min-threshold-bytes = max-threshold-bytes = max-probability = 0
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> slope-enabled <i>boolean</i>

Tree	slope-enabled
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

forwarding-class *keyword*

Description	The list of forwarding classes that map to this queue.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> forwarding-class <i>keyword</i>
Tree	forwarding-class
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

queue-depth

Description	Enter the queue-depth context
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-depth
Tree	queue-depth
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

high-threshold-bytes *number*

Description	The operational hardware value of the high threshold in bytes.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-depth high-threshold-bytes <i>number</i>
Tree	high-threshold-bytes
Units	bytes

Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

last-high-threshold-time *string*

Description	The last time the queue depth exceeded the high-threshold in a rising direction.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-depth last-high-threshold-time <i>string</i>
Tree	last-high-threshold-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

maximum-burst-size *number*

Description	Maximum queue depth in bytes.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> queue-depth maximum-burst-size <i>number</i>
Tree	maximum-burst-size
Units	bytes
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

scheduling

Description	Container for queue scheduling parameters
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> scheduling
Tree	scheduling
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

peak-rate-bps *number*

Description	The actual/operational peak rate in bits per second.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> scheduling peak-rate-bps <i>number</i>
Tree	peak-rate-bps

Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

peak-rate-percent *number*

Description	The maximum percentage of port bandwidth that is available to the traffic in this unicast queue during the PIR scheduling loop. The default is 100.
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> scheduling peak-rate-percent <i>number</i>
Tree	peak-rate-percent
Range	1 to 100
Default	100
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

scheduler-node *reference*

Description	The scheduler node to which the unicast queue is connected. The mappings are fixed and not user-configurable. J2: queue-id 0-7 -> node 1 TD3 (D2/D3): queue-id 0 -> node 0 queue-id 1 -> node 1 queue-id 2 -> node 2 queue-id 3 -> node 3 queue-id 4 -> node 4 queue-id 5 -> node 5 queue-id 6 -> node 6 queue-id 7 -> node 7 TH3: queue-id 0 -> node 1 queue-id 1 -> node 2 queue-id 2 -> node 4 queue-id 3 -> node 5 queue-id 4 -> node 7 queue-id 5 -> node 8 queue-id 6 -> node 10 queue-id 7 -> node 11
Context	interface name <i>string</i> qos output unicast-queue queue-id <i>number</i> scheduling scheduler-node <i>reference</i>
Tree	scheduler-node
Reference	interface name <i>string</i> qos output scheduler tier level <i>number</i> node node-number <i>number</i>
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

strict-priority *boolean*

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.
--------------------	---

Context	interface name <i>string</i> qos output unicast-queue queue-id number scheduling strict-priority <i>boolean</i>
Tree	strict-priority
Default	true
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

weight *number*

Description	Configures the relative weight of a DWRR queue.
Context	interface name <i>string</i> qos output unicast-queue queue-id number scheduling weight <i>number</i>
Tree	weight
Range	1 to 255
Default	1
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

template *reference*

Description	The name of a queue-template to apply to the unicast queue. If a queue has no queue-template, the default queue-template is applied. The user cannot modify the default queue-template.
Context	interface name <i>string</i> qos output unicast-queue queue-id number template reference
Tree	template
Reference	qos queue-templates queue-template name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

voq-template *reference*

Description	The name of a queue-template to apply to the set of associated VOQs. If a queue has no voq-template, the default queue-template is applied
Context	interface name <i>string</i> qos output unicast-queue queue-id number voq-template reference
Tree	voq-template

Reference	qos queue-templates queue-template name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

queue-statistics

Description	Enter the queue-statistics context
Context	interface name <i>string</i> queue-statistics
Tree	queue-statistics
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

multicast-queue [queue-id](#) *number*

Description	List of multicast queues.
Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i>
Tree	multicast-queue
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

queue-id *number*

Description	The queue identifier For J2 and TD3 there is a one-to-one mapping between queue-id and forwarding class. fc0 traffic always use queue-id 0, fc1 traffic always uses queue-id 1, etc. For TH3 the multicast queue-id range is limited to 0-3 and the mapping is as follows: fc0+1 -> queue-id 0 fc2+3 -> queue-id 1 fc4+5 -> queue-id 2 fc6+7 -> queue-id 3
Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i>
Range	0 to 7
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

final-dropped-octets *number*

Description	Number of octets dropped by the multicast queue.
--------------------	--

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
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

final-dropped-packets *number*

Description	Number of packets dropped by the multicast queue.
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
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

last-clear *string*

Description	Timestamp of the last time the statistics associated with this multicast queue were cleared
Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

transmitted-octets *number*

Description	Number of octets transmitted by the multicast queue.
Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> transmitted-octets <i>number</i>
Tree	transmitted-octets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

transmitted-packets *number*

Description	Number of packets transmitted by the multicast queue.
Context	interface name <i>string</i> queue-statistics multicast-queue queue-id <i>number</i> transmitted-packets <i>number</i>
Tree	transmitted-packets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

unicast-queue [queue-id](#) *number*

Description	List of unicast queues.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i>
Tree	unicast-queue
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

queue-id *number*

Description	The queue identifier For unicast traffic on all platforms there is a one-to-one mapping between queue-id and forwarding class. fc0 traffic always use queue-id 0, fc1 traffic always uses queue-id 1, etc.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i>
Range	0 to 7
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

final-dropped-octets *number*

Description	Number of octets 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.
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

Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

final-dropped-packets *number*

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.
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
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

last-clear *string*

Description	Timestamp of the last time the statistics associated with this unicast queue were cleared
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

transmitted-octets *number*

Description	Number of octets transmitted by the unicast queue.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> transmitted-octets <i>number</i>
Tree	transmitted-octets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

transmitted-packets *number*

Description	Number of packets transmitted by the unicast queue, including transit traffic and locally originated traffic.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> transmitted-packets <i>number</i>
Tree	transmitted-packets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

virtual-output-queue [slot](#) *number*

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.
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
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

slot *number*

Description	The slot identifier for the virtual output queue.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i>
Range	1 to 8
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

dropped-octets

Description	Enter the dropped-octets context
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-octets
Tree	dropped-octets
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

high-drop-probability *number*

Description The number of octets in unicast packets dropped in the VOQ due to the congestion at the egress port/queue that were classified as high drop-probability. 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.

Context [interface name](#) *string* [queue-statistics unicast-queue queue-id](#) *number* [virtual-output-queue slot](#) *number* [dropped-octets high-drop-probability](#) *number*

Tree [high-drop-probability](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

low-drop-probability *number*

Description The number of octets in unicast packets dropped in the VOQ due to the congestion at the egress port/queue that were classified as low drop-probability. 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.

Context [interface name](#) *string* [queue-statistics unicast-queue queue-id](#) *number* [virtual-output-queue slot](#) *number* [dropped-octets low-drop-probability](#) *number*

Tree [low-drop-probability](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

medium-drop-probability *number*

Description The number of octets in unicast packets dropped in the VOQ due to the congestion at the egress port/queue that were classified as medium drop-probability. 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.

Context [interface name](#) *string* [queue-statistics unicast-queue queue-id](#) *number* [virtual-output-queue slot](#) *number* [dropped-octets medium-drop-probability](#) *number*

Tree [medium-drop-probability](#)

Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

dropped-packets

Description	Enter the dropped-packets context
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-packets
Tree	dropped-packets
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

high-drop-probability *number*

Description	The number of unicast packets dropped in the VOQ due to the congestion at the egress port/queue that were classified as high drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-packets high-drop-probability <i>number</i>
Tree	high-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

low-drop-probability *number*

Description	The number of unicast packets dropped in the VOQ due to the congestion at the egress port/queue that were classified as low drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-packets low-drop-probability <i>number</i>
Tree	low-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

medium-drop-probability *number*

Description	The number of unicast packets dropped in the VOQ due to the congestion at the egress port/queue that were classified as medium drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> dropped-packets medium-drop-probability <i>number</i>
Tree	medium-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

forwarded-octets

Description	Enter the forwarded-octets context
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-octets
Tree	forwarded-octets
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

high-drop-probability *number*

Description	The number of octets in unicast packets transmitted from the VOQ to the egress queue that were classified as high drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-octets high-drop-probability <i>number</i>
Tree	high-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

low-drop-probability number

Description	The number of octets in unicast packets transmitted from the VOQ to the egress queue that were classified as low drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id number virtual-output-queue slot number forwarded-octets low-drop-probability number
Tree	low-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

medium-drop-probability number

Description	The number of octets in unicast packets transmitted from the VOQ to the egress queue that were classified as medium drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id number virtual-output-queue slot number forwarded-octets medium-drop-probability number
Tree	medium-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

forwarded-packets

Description	Enter the forwarded-packets context
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id number virtual-output-queue slot number forwarded-packets
Tree	forwarded-packets
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

high-drop-probability number

Description	The number of unicast packets transmitted from the VOQ to the egress queue that were classified as high drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-packets high-drop-probability <i>number</i>
Tree	high-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

low-drop-probability *number*

Description	The number of unicast packets transmitted from the VOQ to the egress queue that were classified as low drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-packets low-drop-probability <i>number</i>
Tree	low-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

medium-drop-probability *number*

Description	The number of unicast packets transmitted from the VOQ to the egress queue that were classified as medium drop-probability. 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.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> forwarded-packets medium-drop-probability <i>number</i>
Tree	medium-drop-probability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

queue-depth

Description	Enter the queue-depth context
--------------------	-------------------------------

Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> queue-depth
Tree	queue-depth
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

high-threshold-bytes *number*

Description	The operational hardware value of the high threshold in bytes.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> queue-depth high-threshold-bytes <i>number</i>
Tree	high-threshold-bytes
Units	bytes
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-high-threshold-time *string*

Description	The last time the depth of either VOQ associated with this slot exceeded the high-threshold in a rising direction.
Context	interface name <i>string</i> queue-statistics unicast-queue queue-id <i>number</i> virtual-output-queue slot <i>number</i> queue-depth last-high-threshold-time <i>string</i>
Tree	last-high-threshold-time
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sflow

Description	Context to configure sFlow parameters
Context	interface name <i>string</i> sflow
Tree	sflow
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable sFlow on this interface
--------------------	--

Context	interface name <i>string</i> sflow admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

carrier-transitions *number*

Description	Number of times the interface state has transitioned from down to up since the time the device restarted or the last clear.
Context	interface name <i>string</i> statistics carrier-transitions <i>number</i>
Tree	carrier-transitions
Default	0
Configurable	False
Platforms	Supported on all platforms

in-broadcast-packets *number*

Description	Corresponds to ifHCInBroadcastPkts from the IF-MIB.
Context	interface name <i>string</i> statistics in-broadcast-packets <i>number</i>
Tree	in-broadcast-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-discarded-packets *number*

Description	Corresponds to ifInDiscards from the IFMIB. This counts the number of IP packets discarded due to VLAN mismatch, unknown dest MAC or drop by system-filter drop action.
Context	interface name <i>string</i> statistics in-discarded-packets <i>number</i>
Tree	in-discarded-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-error-packets *number*

Description	Corresponds to ifInErrors from the IF-MIB.
Context	interface name <i>string</i> statistics in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-fcs-error-packets *number*

Description	Ingress FCS errors.
Context	interface name <i>string</i> statistics in-fcs-error-packets <i>number</i>
Tree	in-fcs-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-multicast-packets *number*

Description	Corresponds to ifHCInMulticastPkts from the IF-MIB.
Context	interface name <i>string</i> statistics in-multicast-packets <i>number</i>
Tree	in-multicast-packets
Default	0
Configurable	False

Platforms Supported on all platforms

in-octets *number*

Description Corresponds to ifHCInOctets from the IFMIB.
Context [interface name](#) *string* [statistics in-octets](#) *number*
Tree [in-octets](#)
Default 0
Configurable False
Platforms Supported on all platforms

in-unicast-packets *number*

Description Corresponds to ifHCInUcastPkts from the IF-MIB.
Context [interface name](#) *string* [statistics in-unicast-packets](#) *number*
Tree [in-unicast-packets](#)
Default 0
Configurable False
Platforms Supported on all platforms

last-clear *string*

Description Timestamp of the last time the interface counters were cleared.
Context [interface name](#) *string* [statistics last-clear](#) *string*
Tree [last-clear](#)
String Length 20 to 32
Configurable False
Platforms Supported on all platforms

out-broadcast-packets *number*

Description Corresponds to ifHCOutBroadcastPkts from the IF-MIB.
Context [interface name](#) *string* [statistics out-broadcast-packets](#) *number*
Tree [out-broadcast-packets](#)
Default 0
Configurable False

Platforms Supported on all platforms

out-discarded-packets *number*

Description Corresponds to ifOutDiscards from the IF-MIB.
On Jericho2 systems this counts packets dropped by an egress IP ACL of any of the port's subinterfaces.

Context [interface name](#) *string* [statistics](#) [out-discarded-packets](#) *number*

Tree [out-discarded-packets](#)

Default 0

Configurable False

Platforms Supported on all platforms

out-error-packets *number*

Description Corresponds to ifOutErrors from the IF-MIB.

Context [interface name](#) *string* [statistics](#) [out-error-packets](#) *number*

Tree [out-error-packets](#)

Default 0

Configurable False

Platforms Supported on all platforms

out-mirror-octets *number*

Description This counts the number of outgoing mirrored octets

Context [interface name](#) *string* [statistics](#) [out-mirror-octets](#) *number*

Tree [out-mirror-octets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

out-mirror-packets *number*

Description This counts the number of outgoing mirrored packets

Context [interface name](#) *string* [statistics](#) [out-mirror-packets](#) *number*

Tree [out-mirror-packets](#)

Default 0

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

out-multicast-packets *number*

Description	Corresponds to ifHCOutMulticastPkts from the IF-MIB.
Context	interface name <i>string</i> statistics out-multicast-packets <i>number</i>
Tree	out-multicast-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-octets *number*

Description	Corresponds to ifHCOutOctets from the IF-MIB.
Context	interface name <i>string</i> statistics out-octets <i>number</i>
Tree	out-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-unicast-packets *number*

Description	Corresponds to ifHCOutUcastPkts from the IF-MIB.
Context	interface name <i>string</i> statistics out-unicast-packets <i>number</i>
Tree	out-unicast-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

subinterface [index](#) *number*

Description	The list of subinterfaces (logical interfaces) associated with a physical interface
Context	interface name <i>string</i> subinterface index <i>number</i>
Tree	subinterface
Configurable	True

Platforms	Supported on all platforms
Max. Elements	4095

index number

Description	The index of the subinterface, or logical interface number
Context	interface name <i>string</i> subinterface index number
Range	0 to 9999
Configurable	True
Platforms	Supported on all platforms

acl

Description	Container for ACL policies applied to the subinterface
Context	interface name <i>string</i> subinterface index number acl
Tree	acl
Configurable	True
Platforms	Supported on all platforms

input

Description	Container for ACL options that apply to ingress traffic on the subinterface
Context	interface name <i>string</i> subinterface index number acl input
Tree	input
Configurable	True
Platforms	Supported on all platforms

ipv4-filter reference

Description	IPv4 ACL filter to be applied on this interface
Context	interface name <i>string</i> subinterface index number acl input ipv4-filter reference
Tree	ipv4-filter
Reference	acl ipv4-filter name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

ipv6-filter reference

Description	IPv6 ACL filter to be applied on this interface
Context	interface name <i>string</i> subinterface index <i>number</i> acl input ipv6-filter reference
Tree	ipv6-filter
Reference	acl ipv6-filter name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

mac-filter reference

Description	MAC filter to be applied on this interface
Context	interface name <i>string</i> subinterface index <i>number</i> acl input mac-filter reference
Tree	mac-filter
Reference	acl mac-filter name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

output

Description	Container for ACL options that apply to egress traffic on the subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> acl output
Tree	output
Configurable	True
Platforms	Supported on all platforms

ipv4-filter reference

Description	IPv4 ACL filter to be applied on this interface
Context	interface name <i>string</i> subinterface index <i>number</i> acl output ipv4-filter reference
Tree	ipv4-filter
Reference	acl ipv4-filter name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

ipv6-filter *reference*

Description	IPv6 ACL filter to be applied on this interface
Context	interface name <i>string</i> subinterface index <i>number</i> acl output ipv6-filter reference
Tree	ipv6-filter
Reference	acl ipv6-filter name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

mac-filter *reference*

Description	MAC filter to be applied on this interface
Context	interface name <i>string</i> subinterface index <i>number</i> acl output mac-filter reference
Tree	mac-filter
Reference	acl mac-filter name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

admin-state *keyword*

Description	The configured, desired state of the subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

anycast-gw

Description	Enable the anycast-gw context
Context	interface name <i>string</i> subinterface index <i>number</i> anycast-gw
Tree	anycast-gw
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

anycast-gw-mac *string*

Description The MAC address of associated to the anycast-gw IP address.
If the anycast-gw MAC address is not configured, it will be auto-derived from the virtual-router-id value as per draft-ietf-bess-evpn-inter-subnet-forwarding following the format 00:00:5E:00:01:VRID.

Context [interface name](#) *string* [subinterface index](#) *number* [anycast-gw](#) [anycast-gw-mac](#) *string*

Tree [anycast-gw-mac](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

anycast-gw-mac-origin *keyword*

Description Origin of the active anycast-gateway MAC address.
If not configured, the anycast-gateway-mac will be auto-derived out of 00:00:5E:00:01:VRID, where VRID is the Virtual Router Identifier of the subinterface anycast-gw.

Context [interface name](#) *string* [subinterface index](#) *number* [anycast-gw](#) [anycast-gw-mac-origin](#) *keyword*

Tree [anycast-gw-mac-origin](#)

Options

- configured
- vrid-auto-derived

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

virtual-router-id *number*

Description The Virtual Router Identifier (VRID) value used to auto-derive the anycast-gw-mac in the format 00:00:5E:00:01:VRID.

Context [interface name](#) *string* [subinterface index](#) *number* [anycast-gw](#) [virtual-router-id](#) *number*

Tree [virtual-router-id](#)

Range 1 to 255

Default 1

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

bridge-table

Description Enable the Bridge Table on the subinterface and configure associated parameters

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table](#)

Tree [bridge-table](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

discard-unknown-src-mac *boolean*

Description Discard frames with unknown source mac addresses. The source mac address of the discarded frame is never learned when this command is enabled.

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table](#) [discard-unknown-src-mac](#) *boolean*

Tree [discard-unknown-src-mac](#)

Default false

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-duplication

Description Enter the mac-duplication context

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table](#) [mac-duplication](#)

Tree [mac-duplication](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action *keyword*

Description Action to take on the subinterface upon detecting at least one mac addresses as duplicate on the subinterface. In particular:

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table](#) [mac-duplication](#) [action](#) *keyword*

Tree [action](#)

Default	use-net-instance-action
Options	<ul style="list-style-type: none"> • use-net-instance-action • stop-learning • blackhole • oper-down
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

duplicate-entries

Description	Enter the duplicate-entries context
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication duplicate-entries
Tree	duplicate-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac *address string*

Description	MACs duplicated on the bridging instance
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address *string*

Description	Enter the address context
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dup-detect-time *string*

Description	The date and time when the mac was declared duplicate
--------------------	---

Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> dup-detect-time <i>string</i>
Tree	dup-detect-time
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

hold-down-time-remaining (*keyword* | *number*)

Description	Remaining hold down time for duplicate MAC
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> hold-down-time-remaining (<i>keyword</i> <i>number</i>)
Tree	hold-down-time-remaining
Units	seconds
Options	<ul style="list-style-type: none"> indefinite
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-learning

Description	Enter the mac-learning context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-learning
Tree	mac-learning
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

admin-state *keyword*

Description	Configurable state of the learning procedures for dynamic mac addresses. If disabled, the existing macs in the bridge-table will be kept (and refreshed if new frames arrive for them) but no new mac addresses will be learned. Frames with unknown mac addresses are not dropped, unless discard-unknown-src-mac is configured.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-learning admin-state <i>keyword</i>
Tree	admin-state
Default	enable

Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

aging

Description	Enter the aging context
Context	interface name <i>string</i> subinterface <i>index number</i> bridge-table mac-learning aging
Tree	aging
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

admin-state *keyword*

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.
Context	interface name <i>string</i> subinterface <i>index number</i> bridge-table mac-learning aging admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

learnt-entries

Description	Enter the learnt-entries context
Context	interface name <i>string</i> subinterface <i>index number</i> bridge-table mac-learning learnt-entries
Tree	learnt-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac address string

Description	MACs learnt on the bridging instance
Context	interface name string subinterface index number bridge-table mac-learning learnt-entries mac address string
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Enter the address context
Context	interface name string subinterface index number bridge-table mac-learning learnt-entries mac address string
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

aging (number | keyword)

Description	Remaining age time for learnt MACs
Context	interface name string subinterface index number bridge-table mac-learning learnt-entries mac address string aging (number keyword)
Tree	aging
Units	seconds
Options	<ul style="list-style-type: none"> disabled
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-update string

Description	The date and time of the last update of this learnt MAC
Context	interface name string subinterface index number bridge-table mac-learning learnt-entries mac address string last-update string
Tree	last-update
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-limit

Description	Bridge Table size and thresholds.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-limit
Tree	mac-limit
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

maximum-entries *number*

Description	Maximum number of MAC addresses allowed in the bridge-table.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-limit maximum-entries <i>number</i>
Tree	maximum-entries
Range	1 to 8192
Default	250
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

warning-threshold-pct *number*

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%
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Range	6 to 100
Default	95
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-table

Description	Enter the mac-table context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-table
Tree	mac-table
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac address string

Description MACs learnt on the bridging instance

Context [interface name string](#) [subinterface index number](#) [bridge-table mac-table mac address string](#)

Tree [mac](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description Enter the address context

Context [interface name string](#) [subinterface index number](#) [bridge-table mac-table mac address string](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

failed-slots number

Description The list of slot IDs corresponding to the linecards that did not successfully program the mac

Context [interface name string](#) [subinterface index number](#) [bridge-table mac-table mac address string](#) [failed-slots number](#)

Tree [failed-slots](#)

Range 1 to 8

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-update string

Description The date and time of the last update of this MAC

Context [interface name string](#) [subinterface index number](#) [bridge-table mac-table mac address string](#) [last-update string](#)

Tree [last-update](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

not-programmed-reason *keyword*

Description The reason why the MAC is not programmed

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table mac-table mac address](#) *string* **not-programmed-reason** *keyword*

Tree [not-programmed-reason](#)

Options

- mac-limit
- failed-on-slots
- no-destination-index
- reserved

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

type *keyword*

Description The type of the MAC installed in the fib.

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table mac-table mac address](#) *string* **type** *keyword*

Tree [type](#)

Options

- static
- duplicate
- learnt
- irb-interface
- evpn
- evpn-static
- irb-interface-anycast
- proxy-anti-spoof
- reserved
- eth-cfm
- roe

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

active-entries *number*

Description	The total number of entries that are active on the sub-interface.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

failed-entries *number*

Description	The total number of MACs, which have not been programmed on atleast one slot
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-type *type* *keyword*

Description	The type of the MAC on the sub-interface.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics mac-type <i>type</i> <i>keyword</i>
Tree	mac-type
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

type *keyword*

Description	Enter the type context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics mac-type <i>type</i> <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

active-entries *number*

Description	The total number of entries of this type on the sub-interface
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics mac-type <i>type</i> <i>keyword</i> active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

failed-entries *number*

Description	The total number of MACs of this type, which have not been programmed on atleast one slot
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table statistics mac-type <i>type</i> <i>keyword</i> failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-entries *number*

Description The total number of MACs of this type, active and inactive, on the sub-interface.

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table statistics mac-type type](#) *keyword* [total-entries](#) *number*

Tree [total-entries](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-entries *number*

Description The total number of MACs, active and inactive, on the sub-interface.

Context [interface name](#) *string* [subinterface index](#) *number* [bridge-table statistics total-entries](#) *number*

Tree [total-entries](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description *string*

Description A user-configured description of the interface

Context [interface name](#) *string* [subinterface index](#) *number* [description](#) *string*

Tree [description](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

ethernet-segment-association

Description ethernet-segment association information.

Context [interface name](#) *string* [subinterface index](#) *number* [ethernet-segment-association](#)

Tree [ethernet-segment-association](#)

Configurable	False
Platforms	Supported on all platforms

designated-forwarder *boolean*

Description	The value of this leaf indicates if the interface is the designated forwarder for the ethernet-segment on the network-instance.
Context	interface name <i>string</i> subinterface index <i>number</i> ethernet-segment-association designated-forwarder <i>boolean</i>
Tree	designated-forwarder
Default	false
Configurable	False
Platforms	Supported on all platforms

es-managed *boolean*

Description	The value of this leaf indicates if the interface is managed by the ethernet-segment on the network-instance.
Context	interface name <i>string</i> subinterface index <i>number</i> ethernet-segment-association es-managed <i>boolean</i>
Tree	es-managed
Default	false
Configurable	False
Platforms	Supported on all platforms

ethernet-segment *string*

Description	The value of this leaf indicates the ethernet-segment, the sub-interface is associated to.
Context	interface name <i>string</i> subinterface index <i>number</i> ethernet-segment-association ethernet-segment <i>string</i>
Tree	ethernet-segment
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

ifindex number

Description	System-wide persistent unique ifIndex assigned to the subinterface
Context	interface name <i>string</i> subinterface <i>index number</i> ifindex <i>number</i>
Tree	ifindex
Configurable	False
Platforms	Supported on all platforms

ip-mtu number

Description	<p>IP MTU of the subinterface in bytes, including the IP header but excluding Ethernet encapsulation</p> <p>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.</p> <p>The default IP MTU for a subinterface is taken from /system/mtu/default-ip-mtu. For the mgmt0 and mgmt0-standby subinterfaces the default is the associated interface MTU minus the Ethernet encapsulation overhead.</p> <p>The IP MTU is not configurable for subinterfaces of loopback interfaces.</p> <p>The 7220 IXR-D1, 7220 IXR-D2, 7220 IXR-D3, 7220 IXR-H2, and 7220 IXR-H3 systems support a maximum IP MTU of 9398 bytes.</p> <p>Each 7250 IXR IMM supports a maximum of 4 different IP MTU values. 7220 IXR systems do not have any limit on the maximum number of different IP MTU values.</p>
Context	interface name <i>string</i> subinterface <i>index number</i> ip-mtu <i>number</i>
Tree	ip-mtu
Range	1280 to 9486
Units	bytes
Configurable	True
Platforms	Supported on all platforms

ipv4

Description	<p>Enable IPv4 on the subinterface and configure associated parameters</p> <p>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.</p>
Context	interface name <i>string</i> subinterface <i>index number</i> ipv4

Tree	ipv4
Configurable	True
Platforms	Supported on all platforms

address [ip-prefix](#) *string*

Description	The list of IPv4 addresses assigned to the subinterface.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 address ip-prefix <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms
Max. Elements	64

[ip-prefix](#) *string*

Description	The IPv4 address and prefix length in CIDR notation Subnets on the same subinterface are allowed to overlap as long as the host bits are different. When a locally originated unicast packet is destined to a host covered by multiple subnets associated with a subinterface, the source address is chosen to be the numerically lowest IP address among all these subnets. For example, if the addresses 172.16.1.1/12, 172.16.1.2/12, and 172.16.1.3/12 are configured on the same interface, 172.16.1.1 would be used as a local address when you issue a ping 172.16.1.5 command
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 address ip-prefix <i>string</i>
Configurable	True
Platforms	Supported on all platforms

[anycast-gw](#) *boolean*

Description	This designates the associated IPv4 address as an anycast-gateway IPv4 address of the subinterface. When this parameter is set to true:
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 address ip-prefix <i>string</i> anycast-gw <i>boolean</i>
Tree	anycast-gw
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

origin *keyword*

Description	The origin of the IPv4 address.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> origin <i>keyword</i>
Tree	origin
Options	<ul style="list-style-type: none"> • other • static • dhcp • link-layer • random
Configurable	False
Platforms	Supported on all platforms

primary

Description	<p>One of the IPv4 prefixes assigned to the subinterface can be explicitly configured as primary by setting this leaf to true. This designates the associated IPv4 address as a primary IPv4 address of the subinterface. By default, the numerically lowest value IPv4 address is selected as the primary address.</p> <p>The primary address is used as the source address for locally originated broadcast and multicast packets sent out the subinterface.</p>
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> primary
Tree	primary
Configurable	True
Platforms	Supported on all platforms

status *keyword*

Description	The status of an IPv4 address
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 address ip-prefix <i>string</i> status <i>keyword</i>
Tree	status
Options	<ul style="list-style-type: none"> • preferred • inaccessible • tentative • duplicate

Configurable	False
Platforms	Supported on all platforms

allow-directed-broadcast *boolean*

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>
Context	interface name string subinterface index number ipv4 allow-directed-broadcast <i>boolean</i>
Tree	allow-directed-broadcast
Default	false
Configurable	True
Platforms	Supported on all platforms

arp

Description	Container for the IPv4 ARP protocol
Context	interface name string subinterface index number ipv4 arp
Tree	arp
Configurable	True
Platforms	Supported on all platforms

debug *keyword*

Description	List of events to debug
Context	interface name string subinterface index number ipv4 arp debug <i>keyword</i>

Tree	debug
Options	<ul style="list-style-type: none"> • messages <p>Capture all arp-request and reply-messages sent and received by the subinterface</p>
Configurable	True
Platforms	Supported on all platforms

duplicate-address-detection *boolean*

Description	If set to true IPv4 Address Conflict Detection per RFC 5227 is performed on the IPv4 address assigned to the subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp duplicate-address-detection <i>boolean</i>
Tree	duplicate-address-detection
Default	true
Configurable	True
Platforms	Supported on all platforms

evpn

Description	Configure which types of ARP or ND entries will be advertised in EVPN MAC/IP routes.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp evpn
Tree	evpn
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

advertise [route-type](#) *keyword*

Description	Enter the advertise list instance
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp evpn advertise route-type <i>keyword</i>
Tree	advertise
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

route-type *keyword*

Description	Controls what type of ARP or ND entries to advertise.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp evpn advertise route-type <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • dynamic
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

admin-tag *number*

Description	Configure tag to use with the host route generated from an ARP or ND entry.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp evpn advertise route-type <i>keyword</i> admin-tag <i>number</i>
Tree	admin-tag
Range	0 to 255
Default	0
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

host-route

Description	Configure which types of ARP or ND entries will be populated in the route-table.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp host-route
Tree	host-route
Configurable	True
Platforms	Supported on all platforms

populate [route-type](#) *keyword*

Description	Enter the populate list instance
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp host-route populate route-type <i>keyword</i>
Tree	populate
Configurable	True
Platforms	Supported on all platforms

route-type *keyword*

Description	Controls what type of ARP or ND entries generate a host route.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp host-route populate route-type <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • dynamic • evpn
Configurable	True
Platforms	Supported on all platforms

admin-tag *number*

Description	Configure tag to use with the host route generated from an ARP or ND entry.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp host-route populate route-type <i>keyword</i> admin-tag <i>number</i>
Tree	admin-tag
Range	1 to 255
Configurable	True
Platforms	Supported on all platforms

learn-unsolicited *boolean*

Description	If set to true an ARP entry should be learned from any received ARP packets.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp learn-unsolicited <i>boolean</i>
Tree	learn-unsolicited
Default	false
Configurable	True
Platforms	Supported on all platforms

neighbor [ipv4-address](#) *string*

Description	<p>List of static and dynamic ARP cache entries that map an IPv4 address to a MAC address</p> <p>To configure a static ARP entry a value must be written into this leaf and the link-layer-address leaf.</p>
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>
Tree	neighbor
Configurable	True
Platforms	Supported on all platforms

ipv4-address *string*

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.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

datapath-programming

Description	Container for state related to the datapath programming of the ARP or neighbor entry
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> datapath-programming
Tree	datapath-programming
Configurable	False
Platforms	Supported on all platforms

last-failed-complexes *string*

Description	List of forwarding complexes that reported a failure for the last operation. They appear in the format (slot-number,complex-number).
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> datapath-programming last-failed-complexes <i>string</i>
Tree	last-failed-complexes
Configurable	False
Platforms	Supported on all platforms

status *keyword*

Description	The status of the ARP or neighbor entry with respect to datapath programming
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> datapath-programming status <i>keyword</i>
Tree	status
Options	<ul style="list-style-type: none"> • success All linecard complexes have reported that the entry was programmed successfully • failed At least one linecard complex reported that the entry was not programmed successfully or else this entry was not even provided to the datapath for programming because the system limit on the number of IPv4 ARP and IPv6 neighbor entries was exceeded • pending The ARP or neighbor entry was provided to the datapath for programming but at least one linecard complex has not provided a status yet.
Configurable	False
Platforms	Supported on all platforms

expiration-time *string*

Description	The date and time when the dynamic ARP entry is set to expire
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

link-layer-address *string*

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.
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
Configurable	True

Platforms Supported on all platforms

origin *keyword*

Description The origin of the ARP entry

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp neighbor ipv4-address](#) *string* [origin](#) *keyword*

Tree [origin](#)

Options

- other
- static
- dynamic
- evpn

Configurable False

Platforms Supported on all platforms

proxy-arp *boolean*

Description When set to true, the router replies with its own MAC to ARP Request destined to any host.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp proxy-arp](#) *boolean*

Tree [proxy-arp](#)

Default false

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

timeout *number*

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.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp timeout](#) *number*

Tree [timeout](#)

Range 60 to 65535

Default 14400

Units seconds

Configurable True

Platforms Supported on all platforms

virtual-ipv4-discovery

Description Enable Virtual IPv4 discovery on the subinterface and configure associated parameters
When enabled, the system will attempt to discover the configured virtual IPv4 addresses on the listed bridged subinterfaces.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp](#) [virtual-ipv4-discovery](#)

Tree [virtual-ipv4-discovery](#)

Configurable True

Platforms Supported on all platforms

address [ipv4-address](#) *string*

Description The list of virtual IPv4 addresses to be discovered on the subinterface.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp](#) [virtual-ipv4-discovery](#) [address ipv4-address](#) *string*

Tree [address](#)

Configurable True

Platforms Supported on all platforms

Max. Elements 640

ipv4-address *string*

Description The virtual IPv4 address.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp](#) [virtual-ipv4-discovery](#) [address ipv4-address](#) *string*

Configurable True

Platforms Supported on all platforms

allowed-macs *string*

Description List of allowed mac addresses for a discovered virtual IP address.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv4 arp](#) [virtual-ipv4-discovery](#) [address ipv4-address](#) *string* [allowed-macs](#) *string*

Tree [allowed-macs](#)

Configurable	True
Platforms	Supported on all platforms
Max. Elements	10

probe-bridged-subinterfaces *reference*

Description	Configure the list of bridged sub-interfaces on the associated MAC-VRF to which the ARP probes are sent.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i> probe-bridged-subinterfaces reference
Tree	probe-bridged-subinterfaces
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True
Platforms	Supported on all platforms
Max. Elements	10

probe-interval *number*

Description	Configure the ARP probe interval at which the system sends an ARP request for the virtual IPv4 address. The default value of zero determines that the system sends an ARP Request for the virtual IPv4 only when the address is configured. The creation of the ARP entry for the virtual IPv4 address will in this case rely on the server sending a Gratuitous ARP for the virtual IPv4 address. When the value is set to a non-zero interval, the system sends a periodic ARP Request at the configured interval and irrespective of the ARP entry being already created.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i> probe-interval <i>number</i>
Tree	probe-interval
Range	0 5 to 86400
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Statistics for the Virtual IP address
--------------------	---------------------------------------

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

out-probe-packets *number*

Description	The number of probe packets transmitted for the Virtual IP discovery.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i> statistics out-probe-packets <i>number</i>
Tree	out-probe-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Global statistics for Virtual IP discovery
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp virtual-ipv4-discovery statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

out-total-probe-packets *number*

Description	The number of total probe packets transmitted for Virtual discovery.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 arp virtual-ipv4-discovery statistics out-total-probe-packets <i>number</i>
Tree	out-total-probe-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

dhcp-client

Description	Container for options related to DHCP
--------------------	---------------------------------------

Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-client
Tree	dhcp-client
Configurable	True
Platforms	Supported on all platforms

trace-options

Description	Container for tracing DHCPv4 operations on the subinterface
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-client trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace *keyword*

Description	List of events to trace
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-client trace-options trace <i>keyword</i>
Tree	trace
Options	<ul style="list-style-type: none"> • <code>messages</code> Capture all DHCPv4 messages sent and received by the subinterface
Configurable	True
Platforms	Supported on all platforms

dhcp-relay

Description	Container for options related to DHCPv4 relay
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay
Tree	dhcp-relay
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	The configurable state of the dhcp relay agent
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

gi-address *string*

Description	IPv4 address to be used as giaddr of the relayed packets towards DHCPv4 servers. This address can be any IPv4 address configured within the network-instance towards the DHCPv4 server
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay gi-address <i>string</i>
Tree	gi-address
Configurable	True
Platforms	Supported on all platforms

network-instance *reference*

Description	The network instance to relay dhcp packets to
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay network-instance <i>reference</i>
Tree	network-instance
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The reason causing the dhcp relay agent to go into operational down state
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • dhcp-relay-admin-down • sub-interface-oper-down

	<ul style="list-style-type: none"> • all-dhcp-servers-unreachable-within-net-instance • gi-address-not-matching-relay-sub-interface-ipv4-addresses • no-valid-ipv4-address-on-sub-interface
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of the dhcp relay agent
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting

Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.

- waiting

Component or process is currently waiting

Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

option *keyword*

Description	List of option82 suboptions to insert into relayed packet towards DHCPv4 server
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay option <i>keyword</i>
Tree	option
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
Platforms	Supported on all platforms

server (*ipv4-address* | *domain-name*)

Description	List of the DHCPv4 servers that the DHCPv4 relay function will relay DHCPv4 packets to/from
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay server (<i>ipv4-address</i> <i>domain-name</i>)
Tree	server
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

Max. Elements	8
Min. Elements	1

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

client-packets-discarded *number*

Description	Total discarded dhcp packets from dhcp client(s) towards DHCP server(s)
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay statistics client-packets-discarded <i>number</i>
Tree	client-packets-discarded
Default	0
Configurable	False
Platforms	Supported on all platforms

client-packets-received *number*

Description	Total received dhcp packets from dhcp client(s) for DHCP Relay
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay statistics client-packets-received <i>number</i>
Tree	client-packets-received
Default	0
Configurable	False
Platforms	Supported on all platforms

client-packets-relayed *number*

Description	Total relayed dhcp packets from dhcp client(s) towards DHCP server(s)
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 dhcp-relay statistics client-packets-relayed <i>number</i>
Tree	client-packets-relayed

Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-discarded *number*

Description	Total discarded dhcp packets from DHCP server(s) towards dhcp client(s)
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay statistics server-packets-discarded <i>number</i>
Tree	server-packets-discarded
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-received *number*

Description	Total received dhcp packets from DHCP server(s) for DHCP Relay
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay statistics server-packets-received <i>number</i>
Tree	server-packets-received
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-relayed *number*

Description	Total relayed dhcp packets from DHCP server(s) towards dhcp client(s)
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay statistics server-packets-relayed <i>number</i>
Tree	server-packets-relayed
Default	0
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Container for tracing DHCPv4 relay operations on the subinterface
--------------------	---

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace keyword

Description	List of events to trace
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay trace-options trace <i>keyword</i>
Tree	trace
Options	<ul style="list-style-type: none"> messages Capture all DHCPv4 messages sent and received by the subinterface
Configurable	True
Platforms	Supported on all platforms

use-gi-addr-as-src-ip-addr boolean

Description	When this is set, the configured giaddress will be used as source ip address.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-relay use-gi-addr-as-src-ip-addr <i>boolean</i>
Tree	use-gi-addr-as-src-ip-addr
Default	false
Configurable	True
Platforms	Supported on all platforms

dhcp-server

Description	Enable the dhcp-server context
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 dhcp-server
Tree	dhcp-server
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enables/Disables DHCP server function on subinterface
Context	interface name <i>string</i> subinterface index number ipv4 dhcp-server admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details if the dhcp server is operationally available
Context	interface name <i>string</i> subinterface index number ipv4 dhcp-server oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power

- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

statistics

Description	Container for subinterface statistics, counting IPv4 packets or IPv6 packets or both depending on the context
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics
Tree	statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-discarded-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both (transit and terminating traffic) that were dropped for any of the following reasons: This also includes IP/MPLS packets dropped by ingress interface ACL drop action or CPM filer drop action.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-discarded-packets <i>number</i>
Tree	in-discarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-error-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both discarded due to errors, counting transit and terminating traffic The sum of the following RFC 4293 counters: ipIfStatsInHdrErrors ipIfStatsInNoRoutes ipIfStatsInAddrErrors ipIfStatsInUnknownProtos ipIfStatsInTruncatedPkts
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-forwarded-octets *number*

Description	The number of octets in input IPv4 packets or IPv6 packets or both received on this subinterface and counted in in-forwarded-packets
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-forwarded-octets <i>number</i>
Tree	in-forwarded-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-forwarded-packets *number*

Description	The number of input IPv4 packets or IPv6 packets or both received on this subinterface for which the router was not the final destination and for which the router attempted to find a route to forward them to that final destination. 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. On 7220 IXR systems this also counts received traffic that is terminating.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-forwarded-packets <i>number</i>
Tree	in-forwarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-matched-ra-packets *number*

Description	The total number of IPv6 packets matched with applied RA-Guard policy
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-matched-ra-packets <i>number</i>
Tree	in-matched-ra-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-octets *number*

Description	The total number of octets received in input packets, counting transit and terminating traffic
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-octets <i>number</i>
Tree	in-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-packets *number*

Description	The total number of input packets received, counting transit and terminating traffic This equals the sum of: in-error-packets in-discarded-packets (also includes IP/MPLS packets) in-terminated-packets (also includes IP/MPLS packets) in-forwarded-packets
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-packets <i>number</i>
Tree	in-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-terminated-octets *number*

Description	The total number of octets in input IPv4 packets or IPv6 packets or both that were received on this subinterface and counted in in-terminated-packets
--------------------	---

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-terminated-octets <i>number</i>
Tree	in-terminated-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-terminated-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both 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: This also includes terminating IP/MPLS packets.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics in-terminated-packets <i>number</i>
Tree	in-terminated-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-clear *string*

Description	Timestamp of the last time the subinterface counters were cleared.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-discarded-packets *number*

Description	The total number of IPv4 packets or IPv6 packets or both, originating and transit, sent towards this subinterface that were dropped. This also includes IP/MPLS packets dropped by egress interface ACL drop action.
--------------------	---

Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-discarded-packets <i>number</i>
Tree	out-discarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-error-packets *number*

Description	The number of IPv4 packets or IPv6 packets or both, 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. On 7250 IXR systems this is incremented when the IPv4 packet size exceeds the IP MTU and fragmentation was not allowed or not supported
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-error-packets <i>number</i>
Tree	out-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-octets *number*

Description	The number of octets in transit IPv4 packets or IPv6 packets or both which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-forwarded-octets <i>number</i>
Tree	out-forwarded-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-packets *number*

Description	The number of transit IPv4 packets or IPv6 packets or both which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-forwarded-packets <i>number</i>
Tree	out-forwarded-packets

Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-octets *number*

Description	The total number of octets in IPv4 packets or IPv6 packets or both delivered to the lower layers for transmission
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-octets <i>number</i>
Tree	out-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-originated-octets *number*

Description	The number of octets in IPv4 packets or IPv6 packets or both which originated on the CPM and which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-originated-octets <i>number</i>
Tree	out-originated-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-originated-packets *number*

Description	The number of IPv4 packets or IPv6 packets or both which originated on the CPM and which the router attempted to route out this subinterface This includes all originated ICMP/ICMPv6 messages.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-originated-packets <i>number</i>
Tree	out-originated-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-packets *number*

Description	The total number of IPv4 packets or IPv6 packets or both 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>
Context	interface name <i>string</i> subinterface index <i>number</i> ipv4 statistics out-packets <i>number</i>
Tree	out-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6

Description	Enable IPv6 on the subinterface and configure associated parameters 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:
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6
Tree	ipv6
Configurable	True
Platforms	Supported on all platforms

address [ip-prefix](#) *string*

Description	The list of IPv6 addresses assigned to the subinterface.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms
Max. Elements	18

ip-prefix string

Description	The IPv6 address and prefix-length in CIDR notation Up to 16 global unicast IPv6 addresses can be assigned to each subinterface. Global unicast IPv6 address subnets on the same subinterface are allowed to overlap as long as the host bits are different. When a locally originated unicast packet is destined to a host covered by multiple subnets associated with a subinterface, the source address is chosen to be the numerically lowest IP address among all these subnets.
Context	interface name string subinterface index number ipv6 address ip-prefix string
Configurable	True
Platforms	Supported on all platforms

anycast-gw boolean

Description	This designates the associated IPv6 address as an anycast-gateway IPv6 address of the subinterface. When this parameter is set to true:
Context	interface name string subinterface index number ipv6 address ip-prefix string anycast-gw boolean
Tree	anycast-gw
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

origin keyword

Description	The origin of the IPv6 address
Context	interface name string subinterface index number ipv6 address ip-prefix string origin keyword
Tree	origin
Options	<ul style="list-style-type: none"> • other • static • dhcp • link-layer • random
Configurable	False
Platforms	Supported on all platforms

primary

Description	One of the IPv6 prefixes assigned to the subinterface can be explicitly configured as primary by setting this leaf to true. This designates the associated IPv6 address as a primary IPv6 address of the subinterface. By default, the numerically lowest value IPv6 address is selected as the primary address. The primary address is used as the source address for locally originated broadcast and multicast packets sent out the subinterface.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> primary
Tree	primary
Configurable	True
Platforms	Supported on all platforms

status *keyword*

Description	The status of an IPv6 address
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 address ip-prefix <i>string</i> status <i>keyword</i>
Tree	status
Options	<ul style="list-style-type: none"> • preferred • deprecated • invalid • inaccessible • unknown • tentative • duplicate • optimistic
Configurable	False
Platforms	Supported on all platforms

dhcp-client

Description	Container for options related to DHCPv6
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-client
Tree	dhcp-client
Configurable	True
Platforms	Supported on all platforms

trace-options

Description	Container for tracing DHCPv6 operations on the subinterface
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-client trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace *keyword*

Description	List of events to trace
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-client trace-options trace <i>keyword</i>
Tree	trace
Options	<ul style="list-style-type: none"> • messages Capture all DHCPv6 messages sent and received by the subinterface
Configurable	True
Platforms	Supported on all platforms

dhcp-relay

Description	Container for options related to DHCPv6 relay
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-relay
Tree	dhcp-relay
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	The configurable state of the dhcp relay agent
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-relay admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable

Configurable	True
Platforms	Supported on all platforms

network-instance *reference*

Description	The network instance to relay dhcp packets to
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay network-instance reference
Tree	network-instance
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The reason causing the dhcp relay agent to go into operational down state
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay oper-down-reason keyword
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • dhcp-relay-admin-down • sub-interface-oper-down • all-dhcpv6-servers-unreachable-within-net-instance • source-address-not-matching-relay-sub-interface-ipv6-addresses • no-valid-ipv6-address-on-sub-interface
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of the dhcp relay agent
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

option keyword**Description**

List of options to insert into relayed packet towards DHCPv6 server

Context[interface name](#) [string](#) [subinterface](#) [index](#) [number](#) [ipv6](#) [dhcp-relay](#) [option](#)
[keyword](#)**Tree**[option](#)

Options	<ul style="list-style-type: none"> • interface-id Enable option 18 Interface-Id into relayed packet towards DHCPv6 server, format=system_name/VRF_instance/sub-interface_id:vlan_id • remote-id Enable option 37 Remote Identifier into relayed packet towards DHCPv6 server, format=client MAC address • client-link-layer-address Enable option 79 Client Link-Layer Address into relayed packet towards DHCPv6 server, format based on rfc-6939
Configurable	True
Platforms	Supported on all platforms

server (*ipv6-address* | *domain-name*)

Description	List of the DHCPv6 servers that the DHCPv6 relay function will relay DHCPv6 packets to/from
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay server (<i>ipv6-address</i> <i>domain-name</i>)
Tree	server
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms
Max. Elements	8
Min. Elements	1

source-address *string*

Description	Source IPv6 address of the relayed packets towards DHCPv6 servers this address can be any IPv6 address configured within the network-instance towards the DHCPv6 server
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay source-address <i>string</i>
Tree	source-address
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
--------------------	------------------------------

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

client-packets-discarded *number*

Description	Total discarded dhcp packets from dhcp client(s) towards DHCP server(s)
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics client-packets-discarded <i>number</i>
Tree	client-packets-discarded
Default	0
Configurable	False
Platforms	Supported on all platforms

client-packets-received *number*

Description	Total received dhcp packets from dhcp client(s) for DHCP Relay
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics client-packets-received <i>number</i>
Tree	client-packets-received
Default	0
Configurable	False
Platforms	Supported on all platforms

client-packets-relayed *number*

Description	Total relayed dhcp packets from dhcp client(s) towards DHCP server(s)
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics client-packets-relayed <i>number</i>
Tree	client-packets-relayed
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-discarded *number*

Description	Total discarded dhcp packets from DHCP server(s) towards dhcp client(s)
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics server-packets-discarded <i>number</i>
Tree	server-packets-discarded
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-received *number*

Description	Total received dhcp packets from DHCP server(s) for DHCP Relay
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics server-packets-received <i>number</i>
Tree	server-packets-received
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-relayed *number*

Description	Total relayed dhcp packets from DHCP server(s) towards dhcp client(s)
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay statistics server-packets-relayed <i>number</i>
Tree	server-packets-relayed
Default	0
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Container for tracing DHCPv6 relay operations on the subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 dhcp-relay trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace keyword

Description	List of events to trace
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-relay trace-options trace <i>keyword</i>
Tree	trace
Options	<ul style="list-style-type: none"> • messages Capture all DHCPv6 messages sent and received by the subinterface
Configurable	True
Platforms	Supported on all platforms

dhcpv6-server

Description	Enable the dhcpv6-server context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcpv6-server
Tree	dhcpv6-server
Configurable	True
Platforms	Supported on all platforms

admin-state keyword

Description	Enables/Disables DHCPv6 server function on subinterface
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcpv6-server admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state keyword

Description	Details if the dhcp server is operationally available
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcpv6-server oper-state <i>keyword</i>
Tree	oper-state

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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

neighbor-discovery

Description	Container for the IPv6 Neighbor Discovery protocol
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery
Tree	neighbor-discovery
Configurable	True
Platforms	Supported on all platforms

debug *keyword*

Description	List of events to debug
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery debug <i>keyword</i>
Tree	debug
Options	<ul style="list-style-type: none"> messages Capture all neighbor-solicitation and neighbor-advertisement messages sent and received by the subinterface
Configurable	True
Platforms	Supported on all platforms

duplicate-address-detection *boolean*

Description	<p>Enables Duplicate Address Detection on all tentative addresses</p> <p>This applies to link-local and global unicast addresses. Only one transmission is done; there are no retransmissions.</p> <p>Must be true on an IPv6 subinterface that has dhcp-client enabled.</p>
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery duplicate-address-detection <i>boolean</i>
Tree	duplicate-address-detection
Default	true
Configurable	True
Platforms	Supported on all platforms

evpn

Description	Configure which types of ARP or ND entries will be advertised in EVPN MAC/IP routes.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery evpn

Tree	evpn
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

advertise [route-type](#) *keyword*

Description	Enter the advertise list instance
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery evpn advertise route-type <i>keyword</i>
Tree	advertise
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

[route-type](#) *keyword*

Description	Controls what type of ARP or ND entries to advertise.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery evpn advertise route-type <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • dynamic
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

[admin-tag](#) *number*

Description	Configure tag to use with the host route generated from an ARP or ND entry.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery evpn advertise route-type <i>keyword</i> admin-tag <i>number</i>
Tree	admin-tag
Range	0 to 255
Default	0
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

host-route

Description	Configure which types of ARP or ND entries will be populated in the route-table.
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery host-route
Tree	host-route
Configurable	True
Platforms	Supported on all platforms

populate [route-type](#) *keyword*

Description	Enter the populate list instance
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery host-route populate route-type <i>keyword</i>
Tree	populate
Configurable	True
Platforms	Supported on all platforms

route-type *keyword*

Description	Controls what type of ARP or ND entries generate a host route.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery host-route populate route-type <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • dynamic • evpn
Configurable	True
Platforms	Supported on all platforms

admin-tag *number*

Description	Configure tag to use with the host route generated from an ARP or ND entry.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery host-route populate route-type <i>keyword</i> admin-tag <i>number</i>
Tree	admin-tag
Range	1 to 255
Configurable	True
Platforms	Supported on all platforms

learn-unsolicited *keyword*

Description	Sets if neighbors should be learned from unsolicited neighbor advertisements for global or link local addresses or both.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery learn-unsolicited <i>keyword</i>
Tree	learn-unsolicited
Default	none
Options	<ul style="list-style-type: none"> • none • global • link-local • both
Configurable	True
Platforms	Supported on all platforms

neighbor [ipv6-address](#) *string*

Description	List of static and dynamic ND cache entries that map an IPv6 address to a MAC address
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Tree	neighbor
Configurable	True
Platforms	Supported on all platforms

ipv6-address *string*

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.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

current-state *keyword*

Description	The Neighbor Unreachability Detection state
--------------------	---

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
Options	<ul style="list-style-type: none"> • incomplete • reachable • stale • delay • probe
Configurable	False
Platforms	Supported on all platforms

datapath-programming

Description	Container for state related to the datapath programming of the ARP or neighbor entry
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> datapath-programming
Tree	datapath-programming
Configurable	False
Platforms	Supported on all platforms

last-failed-complexes *string*

Description	List of forwarding complexes that reported a failure for the last operation. They appear in the format (slot-number,complex-number).
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> datapath-programming last-failed-complexes <i>string</i>
Tree	last-failed-complexes
Configurable	False
Platforms	Supported on all platforms

status *keyword*

Description	The status of the ARP or neighbor entry with respect to datapath programming
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i> datapath-programming status <i>keyword</i>
Tree	status

Options	<ul style="list-style-type: none"> • success All linecard complexes have reported that the entry was programmed successfully • failed At least one linecard complex reported that the entry was not programmed successfully or else this entry was not even provided to the datapath for programming because the system limit on the number of IPv4 ARP and IPv6 neighbor entries was exceeded • pending The ARP or neighbor entry was provided to the datapath for programming but at least one linecard complex has not provided a status yet.
Configurable	False
Platforms	Supported on all platforms

is-router *boolean*

Description	Indicates that the neighbor node claims to be a router (R bit in the Neighbor Advertisement message)
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
Configurable	False
Platforms	Supported on all platforms

link-layer-address *string*

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.
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
Configurable	True
Platforms	Supported on all platforms

next-state-time *string*

Description	The date and time when the neighbor state is expected to transition to the next state
--------------------	---

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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

origin *keyword*

Description	The origin of the neighbor cache entry.
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
Options	<ul style="list-style-type: none"> • other • static • dynamic • evpn
Configurable	False
Platforms	Supported on all platforms

proxy-nd *boolean*

Description	When set to true, the router replies with its own MAC to Neighbor Solicitations destined to any host.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery proxy-nd <i>boolean</i>
Tree	proxy-nd
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

reachable-time *number*

Description	<p>The period of time that a dynamic IPv6 neighbor cache entry is considered reachable after a reachability confirmation event</p> <p>After this time expires the neighbor state moves to STALE.</p>
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery reachable-time <i>number</i>

Tree	reachable-time
Range	30 to 3600
Default	30
Units	seconds
Configurable	True
Platforms	Supported on all platforms

stale-time *number*

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.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery stale-time <i>number</i>
Tree	stale-time
Range	60 to 65535
Default	14400
Units	seconds
Configurable	True
Platforms	Supported on all platforms

virtual-ipv6-discovery

Description	Enable Virtual IPv6 discovery on the subinterface and configure associated parameters When enabled, the system will attempt to discover the configured virtual IPv6 addresses on the listed bridged subinterfaces.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery
Tree	virtual-ipv6-discovery
Configurable	True
Platforms	Supported on all platforms

address [ipv6-address](#) *string*

Description	The list of virtual IPv6 addresses to be discovered on the subinterface.
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms
Max. Elements	640

ipv6-address *string*

Description	The virtual IPv6 address.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

allowed-macs *string*

Description	List of allowed MAC addresses for a discovered virtual IP address.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> allowed-macs <i>string</i>
Tree	allowed-macs
Configurable	True
Platforms	Supported on all platforms
Max. Elements	10

probe-bridged-subinterfaces *reference*

Description	Configure the list of bridged sub-interfaces on the associated MAC-VRF to which the NS probes are sent.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> probe-bridged-subinterfaces <i>reference</i>
Tree	probe-bridged-subinterfaces
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True
Platforms	Supported on all platforms
Max. Elements	10

probe-interval *number*

Description	Configure the probe interval at which the system sends a Neighbor Solicitation (NS) for the virtual IPv6 address. The default value of zero determines that the system sends a NS for the virtual IPv6 only when the address is configured. The creation of the Neighbor entry for the virtual IPv6 address will in this case rely on the server sending an unsolicited Neighbor Advertisement for the virtual IPv6 address. When the value is set to a non-zero interval, the system sends a periodic NS at the configured interval and irrespective of the Neighbor entry being already created.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> probe-interval <i>number</i>
Tree	probe-interval
Range	0 5 to 86400
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Statistics for the Virtual IP address
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

out-probe-packets *number*

Description	The number of probe packets transmitted for the Virtual IP discovery.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> statistics out-probe-packets <i>number</i>
Tree	out-probe-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Global statistics for Virtual IP discovery
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

out-total-probe-packets *number*

Description	The number of total probe packets transmitted for Virtual discovery.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery statistics out-total-probe-packets <i>number</i>
Tree	out-total-probe-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

router-advertisement

Description	Container for configuring IPv6 router discovery options
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement
Tree	router-advertisement
Configurable	True
Platforms	Supported on all platforms

debug *keyword*

Description	List of events to debug
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement debug <i>keyword</i>
Tree	debug
Options	<ul style="list-style-type: none"> • messages <p>Capture all router-solicitation and router-advertisement messages sent and received by the subinterface</p>
Configurable	True
Platforms	Supported on all platforms

router-role

Description	IPv6 router advertisement options that apply when the role of the interface is a router interface.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role
Tree	router-role
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the sending of router advertisements on the subinterface.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

current-hop-limit *number*

Description	The current hop limit to advertise in the router advertisement messages.
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
Default	64
Configurable	True
Platforms	Supported on all platforms

ip-mtu *number*

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. If no value is specified the option is not included.
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role ip-mtu <i>number</i>
Tree	ip-mtu
Range	1280 to 9486
Configurable	True
Platforms	Supported on all platforms

managed-configuration-flag *boolean*

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.
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
Default	false
Configurable	True
Platforms	Supported on all platforms

max-advertisement-interval *number*

Description	The maximum 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.
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
Range	4 to 1800
Default	600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

min-advertisement-interval *number*

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.

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
Range	3 to 1350
Default	200
Units	seconds
Configurable	True
Platforms	Supported on all platforms

other-configuration-flag *boolean*

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).
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
Default	false
Configurable	True
Platforms	Supported on all platforms

prefix [ipv6-prefix](#) *string*

Description	The list of IPv6 prefixes to advertise in the router advertisement messages.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i>
Tree	prefix
Configurable	True
Platforms	Supported on all platforms
Max. Elements	16

ipv6-prefix *string*

Description	An IPv6 global unicast address prefix.
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role prefix ipv6-prefix <i>string</i>
Configurable	True
Platforms	Supported on all platforms

autonomous-flag *boolean*

Description	When this is set in the prefix information option hosts can use the prefix for stateless address autoconfiguration (SLAAC).
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
Default	true
Configurable	True
Platforms	Supported on all platforms

on-link-flag *boolean*

Description	When this is set in the prefix information option hosts can use the prefix for on-link determination.
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
Default	true
Configurable	True
Platforms	Supported on all platforms

preferred-lifetime (*keyword* | *number*)

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.
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</i> <i>number</i>)
Tree	preferred-lifetime
Default	604800
Units	seconds
Options	<ul style="list-style-type: none"> infinite

Configurable	True
Platforms	Supported on all platforms

valid-lifetime (*keyword* | *number*)

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.
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</i> <i>number</i>)
Tree	valid-lifetime
Default	2592000
Units	seconds
Options	<ul style="list-style-type: none"> infinite
Configurable	True
Platforms	Supported on all platforms

reachable-time *number*

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.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role reachable-time <i>number</i>
Tree	reachable-time
Range	0 to 3600000
Default	0
Configurable	True
Platforms	Supported on all platforms

retransmit-time *number*

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.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role retransmit-time <i>number</i>
Tree	retransmit-time

Range	0 to 1800000
Default	0
Configurable	True
Platforms	Supported on all platforms

router-lifetime *number*

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.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 router-advertisement router-role router-lifetime <i>number</i>
Tree	router-lifetime
Range	0 to 9000
Default	1800
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Container for subinterface statistics, counting IPv4 packets or IPv6 packets or both depending on the context
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics
Tree	statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-discarded-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both (transit and terminating traffic) that were dropped for any of the following reasons: This also includes IP/MPLS packets dropped by ingress interface ACL drop action or CPM filer drop action.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics in-discarded-packets <i>number</i>
Tree	in-discarded-packets
Default	0
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

in-error-packets *number*

Description The total number of input IPv4 packets or IPv6 packets or both discarded due to errors, counting transit and terminating traffic

The sum of the following RFC 4293 counters: ipIfStatsInHdrErrors ipIfStatsInNoRoutes ipIfStatsInAddrErrors ipIfStatsInUnknownProtos ipIfStatsInTruncatedPkts

Context [interface name](#) *string* [subinterface index](#) *number* [ipv6 statistics in-error-packets](#) *number*

Tree [in-error-packets](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

in-forwarded-octets *number*

Description The number of octets in input IPv4 packets or IPv6 packets or both received on this subinterface and counted in in-forwarded-packets

Context [interface name](#) *string* [subinterface index](#) *number* [ipv6 statistics in-forwarded-octets](#) *number*

Tree [in-forwarded-octets](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

in-forwarded-packets *number*

Description The number of input IPv4 packets or IPv6 packets or both received on this subinterface for which the router was not the final destination and for which the router attempted to find a route to forward them to that final destination.

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.

On 7220 IXR systems this also counts received traffic that is terminating.

Context [interface name](#) *string* [subinterface index](#) *number* [ipv6 statistics in-forwarded-packets](#) *number*

Tree [in-forwarded-packets](#)

Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-matched-ra-packets *number*

Description	The total number of IPv6 packets matched with applied RA-Guard policy
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics in-matched-ra-packets <i>number</i>
Tree	in-matched-ra-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-octets *number*

Description	The total number of octets received in input packets, counting transit and terminating traffic
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics in-octets <i>number</i>
Tree	in-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-packets *number*

Description	The total number of input packets received, counting transit and terminating traffic This equals the sum of: in-error-packets in-discarded-packets (also includes IP/MPLS packets) in-terminated-packets (also includes IP/MPLS packets) in-forwarded-packets
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics in-packets <i>number</i>
Tree	in-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-terminated-octets *number*

Description	The total number of octets in input IPv4 packets or IPv6 packets or both that were received on this subinterface and counted in in-terminated-packets
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics in-terminated-octets <i>number</i>
Tree	in-terminated-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-terminated-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both 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: This also includes terminating IP/MPLS packets.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics in-terminated-packets <i>number</i>
Tree	in-terminated-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-clear *string*

Description	Timestamp of the last time the subinterface counters were cleared.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-discarded-packets *number*

Description	The total number of IPv4 packets or IPv6 packets or both, originating and transit, sent towards this subinterface that were dropped. This also includes IP/MPLS packets dropped by egress interface ACL drop action.
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-discarded-packets <i>number</i>
Tree	out-discarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-error-packets *number*

Description	The number of IPv4 packets or IPv6 packets or both, 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. On 7250 IXR systems this is incremented when the IPv4 packet size exceeds the IP MTU and fragmentation was not allowed or not supported
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-error-packets <i>number</i>
Tree	out-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-octets *number*

Description	The number of octets in transit IPv4 packets or IPv6 packets or both which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-forwarded-octets <i>number</i>
Tree	out-forwarded-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-packets *number*

Description	The number of transit IPv4 packets or IPv6 packets or both which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-forwarded-packets <i>number</i>
Tree	out-forwarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-octets *number*

Description	The total number of octets in IPv4 packets or IPv6 packets or both delivered to the lower layers for transmission
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-octets <i>number</i>
Tree	out-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-originated-octets *number*

Description	The number of octets in IPv4 packets or IPv6 packets or both which originated on the CPM and which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-originated-octets <i>number</i>
Tree	out-originated-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-originated-packets *number*

Description	The number of IPv4 packets or IPv6 packets or both which originated on the CPM and which the router attempted to route out this subinterface This includes all originated ICMP/ICMPv6 messages.
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-originated-packets <i>number</i>
Tree	out-originated-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-packets *number*

Description	<p>The total number of IPv4 packets or IPv6 packets or both that this router supplied to the lower layers for transmission</p> <p>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></p>
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 statistics out-packets <i>number</i>
Tree	out-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

I2-mtu *number*

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 I2-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-I2-mtu. The L2 MTU is only configurable for bridged subinterfaces.</p> <p>The 7220 IXR-D1, 7220 IXR-D2, 7220 IXR-D3, 7220 IXR-H2, and 7220 IXR-H3 systems support a maximum L2 MTU of 9412 bytes.</p>
Context	interface name <i>string</i> subinterface index <i>number</i> I2-mtu <i>number</i>
Tree	I2-mtu
Range	1500 to 9500
Units	bytes
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-change *string*

Description	The date and time of the most recent change to the subinterface state
Context	interface name <i>string</i> subinterface index <i>number</i> last-change <i>string</i>
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

local-mirror-destination

Description	Container for options related to local mirror destination
Context	interface name <i>string</i> subinterface index <i>number</i> local-mirror-destination
Tree	local-mirror-destination
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

admin-state *keyword*

Description	The configurable state of the local mirror destination
Context	interface name <i>string</i> subinterface index <i>number</i> local-mirror-destination admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-state *keyword*

Description	The operational state of the local mirror destination
Context	interface name <i>string</i> subinterface index <i>number</i> local-mirror-destination oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up <p>Component or process is operational</p>

- 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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mpls**Description**

Container for MPLS configuration and state at the subinterface level

Context[interface name](#) *string* [subinterface index](#) *number* [mpls](#)

Tree	mpls
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Container for MPLS-specific subinterface statistics
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics
Tree	statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-discarded-packets *number*

Description	The total number of MPLS packets that were dropped because they were received with forwarded top label having an MPLS TTL value of 1
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics in-discarded-packets <i>number</i>
Tree	in-discarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-error-packets *number*

Description	The total number of MPLS packets that were dropped because they were received with errors that include:
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-forwarded-octets *number*

Description	The number of octets in MPLS packets received on this subinterface that were attempted to be forwarded to another IP or MPLS interface
--------------------	--

Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics in-forwarded-octets <i>number</i>
Tree	in-forwarded-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-forwarded-packets *number*

Description	The number of MPLS packets received on this subinterface that were attempted to be forwarded to another IP or MPLS interface
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics in-forwarded-packets <i>number</i>
Tree	in-forwarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-octets *number*

Description	The total number of octets in input MPLS packets received, not counting MPLS packets discarded due to ACLs or IP/MPLS packets that terminated on this router.
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics in-octets <i>number</i>
Tree	in-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-packets *number*

Description	The total number of input MPLS packets received, not counting MPLS packets discarded due to ACLs or IP/MPLS packets that terminated on this router. This equals the sum of: in-error-packets in-discarded-packets in-forwarded-packets
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics in-packets <i>number</i>

Tree	in-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-clear *string*

Description	Timestamp of the last time the subinterface MPLS counters were cleared.
Context	interface name <i>string</i> subinterface index number mpls statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-error-packets *number*

Description	The number of MPLS packets that could not be transmitted on this subinterface because of an error. For now this only counts transmission errors that result from the MPLS packet size exceeding the MPLS MTU of the subinterface.
Context	interface name <i>string</i> subinterface index number mpls statistics out-error-packets <i>number</i>
Tree	out-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-octets *number*

Description	The number of octets in MPLS packets transmitted on this subinterface. This does not include IP packets that resulted from a PHP pop operation.
Context	interface name <i>string</i> subinterface index number mpls statistics out-forwarded-octets <i>number</i>
Tree	out-forwarded-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-packets *number*

Description	The number of MPLS packets transmitted on this subinterface. This does not include IP packets that resulted from a PHP pop operation.
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics out-forwarded-packets <i>number</i>
Tree	out-forwarded-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-octets *number*

Description	The total number of octets in output MPLS packets transmitted.
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics out-octets <i>number</i>
Tree	out-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-originated-octets *number*

Description	The number of octets in MPLS packets that were originated by this router.
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics out-originated-octets <i>number</i>
Tree	out-originated-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-originated-packets *number*

Description	The number of MPLS packets that were originated by this router.
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics out-originated-packets <i>number</i>
Tree	out-originated-packets
Default	0

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-packets *number*

Description	The total number of output MPLS packets transmitted. This equals out-originated-packets + out-forwarded-packets
Context	interface name <i>string</i> subinterface index <i>number</i> mpls statistics out-packets <i>number</i>
Tree	out-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

mpls-mtu *number*

Description	MPLS MTU of the subinterface in bytes, including the transmitted label stack. MPLS MTU specifies the maximum sized MPLS packet that can be transmitted on the subinterface. If an MPLS packet containing any payload exceeds this size then it is dropped. If the payload of the dropped packet is IPv4 or IPv6 then this may also result in the generation of an ICMP error message that is either tunneled or sent back to the source. The default MPLS MTU for a subinterface is taken from /system/mtu/default-mpls-mtu. The MPLS MTU is not configurable for subinterfaces of loopback interfaces. Each 7250 IXR IMM supports a maximum of 4 different MPLS MTU values.
Context	interface name <i>string</i> subinterface index <i>number</i> mpls-mtu <i>number</i>
Tree	mpls-mtu
Range	1284 to 9496
Units	bytes
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name *string*

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
Context	interface name <i>string</i> subinterface index <i>number</i> name <i>string</i>

Tree	name
Configurable	False
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The first (and possibly only) reason for the subinterface being operationally down
Context	interface name <i>string</i> subinterface index <i>number</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • admin-disabled • port-down • ip-mtu-resource-exceeded • mpls-mtu-resource-exceeded • ip-mtu-too-large • mpls-mtu-too-large • l2-mtu-too-large • no-ip-config • ip-mtu-larger-than-oper-mac-vrf-mtu • irb-mac-address-not-programmed • missing-xdp-state • no-underlay-egress-next-hop-resources • other
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of the subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up • down
Configurable	False
Platforms	Supported on all platforms

qos

Description	Enter the qos context
Context	interface name <i>string</i> subinterface index <i>number</i> qos
Tree	qos
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

input

Description	Enter the input context
Context	interface name <i>string</i> subinterface index <i>number</i> qos input
Tree	input
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

classifiers

Description	Enter the classifiers context
Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers
Tree	classifiers
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dot1p reference

Description	Reference to the name of a dot1p classifier policy.
Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers dot1p reference
Tree	dot1p
Reference	qos classifiers dot1p-policy <i>name</i> <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dscp reference

Description	Reference to the name of a DSCP classifier policy that applies to both IPv4 and IPv6 traffic.
--------------------	---

Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers dscp reference
Tree	dscp
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

ipv4-dscp *reference*

Description	Reference to the name of a DSCP classifier policy that applies only to IPv4 traffic.
Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers ipv4-dscp reference
Tree	ipv4-dscp
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-dscp *reference*

Description	Reference to the name of a DSCP classifier policy that applies only to IPv6 traffic.
Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers ipv6-dscp reference
Tree	ipv6-dscp
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

mpls-traffic-class *reference*

Description	Reference to the name of an MPLS traffic-class classifier policy
Context	interface name <i>string</i> subinterface index <i>number</i> qos input classifiers mpls-traffic-class reference
Tree	mpls-traffic-class
Reference	qos classifiers mpls-traffic-class-policy name <i>string</i>
Configurable	True

Platforms 7250 IXR-10, 7250 IXR-6

policers

Description Container with information about the policers applied to input traffic on the subinterface.

Context [interface name](#) *string* [subinterface index number](#) [qos input policers](#)

Tree [policers](#)

Configurable True

Platforms Supported on all platforms except 7220 IXR-D1

policer *index number*

Description The list of policer instances belonging to the template definition.

Context [interface name](#) *string* [subinterface index number](#) [qos input policers policer index number](#)

Tree [policer](#)

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

index *number*

Description The policer index

Context [interface name](#) *string* [subinterface index number](#) [qos input policers policer index number](#)

Range 1 to 32

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

committed-burst-size *number*

Description The actual/operational maximum CIR bucket depth in bytes as it is programmed into hardware.

Context [interface name](#) *string* [subinterface index number](#) [qos input policers policer index number](#) [committed-burst-size number](#)

Tree [committed-burst-size](#)

Units bytes

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

committed-rate-kbps *number*

Description The actual/operational committed information rate (CIR) of the policer as it is programmed into hardware.

Context [interface name](#) *string* [subinterface index](#) *number* [qos input policers policer index](#) *number* **committed-rate-kbps** *number*

Tree [committed-rate-kbps](#)

Units kbps

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

maximum-burst-size *number*

Description The actual/operational maximum PIR bucket depth in bytes as it is programmed into hardware.

Context [interface name](#) *string* [subinterface index](#) *number* [qos input policers policer index](#) *number* **maximum-burst-size** *number*

Tree [maximum-burst-size](#)

Units bytes

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

peak-rate-kbps *number*

Description The actual/operational peak information rate (PIR) of the policer as it is programmed into hardware.

Context [interface name](#) *string* [subinterface index](#) *number* [qos input policers policer index](#) *number* **peak-rate-kbps** *number*

Tree [peak-rate-kbps](#)

Units kbps

Configurable False

Platforms Supported on all platforms except 7220 IXR-D1

statistics

Description Enter the statistics context

Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

accepted-octets *number*

Description	The number octets in packets that were accepted by the policer, counting all drop-probabilities at policer output Not available in forwarding-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics accepted-octets <i>number</i>
Tree	accepted-octets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

accepted-packets *number*

Description	The number packets that were accepted by the policer, counting all drop-probabilities at policer output Not available in forwarding-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics accepted-packets <i>number</i>
Tree	accepted-packets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

committed-octets *number*

Description	The number octets in packets that were accepted with low drop-probability at policer output Not available in violating-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics committed-octets <i>number</i>
Tree	committed-octets

Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

committed-packets *number*

Description	The number packets that were accepted with low drop-probability at policer output Not available in violating-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics committed-packets <i>number</i>
Tree	committed-packets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

dropped-octets *number*

Description	The number of octets in packets that were dropped by the policer, counting medium and high drop-probabilities at policer output Not available in forwarding-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics dropped-octets <i>number</i>
Tree	dropped-octets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

dropped-packets *number*

Description	The number packets that were dropped by the policer, counting medium and high drop-probabilities at policer output Not available in forwarding-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics dropped-packets <i>number</i>
Tree	dropped-packets
Default	0

Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

exceeding-octets *number*

Description	The number of octets in packets that were accepted with medium drop-probability at policer output Not available in violating-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics exceeding-octets <i>number</i>
Tree	exceeding-octets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

exceeding-packets *number*

Description	The number packets that were accepted with medium drop-probability at policer output Not available in violating-focus mode
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer index <i>number</i> statistics exceeding-packets <i>number</i>
Tree	exceeding-packets
Default	0
Configurable	False
Platforms	Supported on all platforms except 7220 IXR-D1

policer-template *reference*

Description	The name of the policer template applied to input traffic on the subinterface If this is configured but no value is displayed in state information then there were insufficient resources to completely apply the template.
Context	interface name <i>string</i> subinterface index <i>number</i> qos input policers policer-template <i>reference</i>
Tree	policer-template
Reference	qos policer-templates policer-template name <i>string</i>
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

output

Description	Enter the output context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> qos output
Tree	output
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

rewrite-rules

Description	Enter the rewrite-rules context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> qos output rewrite-rules
Tree	rewrite-rules
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dot1p *reference*

Description	Reference to the name of a dot1p rewrite policy.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> qos output rewrite-rules dot1p <i>reference</i>
Tree	dot1p
Reference	qos rewrite-rules dot1p-policy <i>name</i> <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dscp *reference*

Description	Reference to the name of a DSCP rewrite-rule policy that applies to both IPv4 and IPv6 traffic.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> qos output rewrite-rules dscp <i>reference</i>
Tree	dscp
Reference	qos rewrite-rules dscp-policy <i>name</i> <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

ipv4-dscp reference

Description	Reference to the name of a DSCP rewrite-rule policy that applies only to IPv4 traffic.
Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules ipv4-dscp reference
Tree	ipv4-dscp
Reference	qos rewrite-rules dscp-policy name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-dscp reference

Description	Reference to the name of a DSCP rewrite-rule policy that applies only to IPv6 traffic.
Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules ipv6-dscp reference
Tree	ipv6-dscp
Reference	qos rewrite-rules dscp-policy name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

mpls-traffic-class reference

Description	Reference to the name of an MPLS traffic-class rewrite-rule policy
Context	interface name <i>string</i> subinterface index <i>number</i> qos output rewrite-rules mpls-traffic-class reference
Tree	mpls-traffic-class
Reference	qos rewrite-rules mpls-traffic-class-policy name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ra-guard

Description	Enable the ra-guard context
Context	interface name <i>string</i> subinterface index <i>number</i> ra-guard
Tree	ra-guard
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

policy reference

Description Reference to RA Guard Policy to apply to the associated subinterface

Context [interface name](#) *string* [subinterface index](#) *number* [ra-guard policy reference](#)

Tree [policy](#)

Reference [system ra-guard-policy name](#) *string*

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

vlan-list [vlan-id](#) *number*

Description List of VLAN IDs that the RA policy should be matched against

Context [interface name](#) *string* [subinterface index](#) *number* [ra-guard vlan-list vlan-id number](#)

Tree [vlan-list](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

vlan-id *number*

Description Enter the vlan-id context

Context [interface name](#) *string* [subinterface index](#) *number* [ra-guard vlan-list vlan-id number](#)

Range 0 to 4095

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description Container for subinterface statistics, counting IPv4 packets or IPv6 packets or both depending on the context

Context [interface name](#) *string* [subinterface index](#) *number* [statistics](#)

Tree [statistics](#)

Configurable False

Platforms Supported on all platforms

in-discarded-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both (transit and terminating traffic) that were dropped for any of the following reasons: This also includes IP/MPLS packets dropped by ingress interface ACL drop action or CPM filer drop action.
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-discarded-packets <i>number</i>
Tree	in-discarded-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-error-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both discarded due to errors, counting transit and terminating traffic The sum of the following RFC 4293 counters: ipIfStatsInHdrErrors ipIfStatsInNoRoutes ipIfStatsInAddrErrors ipIfStatsInUnknownProtos ipIfStatsInTruncatedPkts
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-forwarded-octets *number*

Description	The number of octets in input IPv4 packets or IPv6 packets or both received on this subinterface and counted in in-forwarded-packets
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-forwarded-octets <i>number</i>
Tree	in-forwarded-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-forwarded-packets *number*

Description	The number of input IPv4 packets or IPv6 packets or both received on this subinterface for which the router was not the final destination and for which the router attempted to find a route to forward them to that final destination. 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. On 7220 IXR systems this also counts received traffic that is terminating.
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-forwarded-packets <i>number</i>
Tree	in-forwarded-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-matched-ra-packets *number*

Description	The total number of IPv6 packets matched with applied RA-Guard policy
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-matched-ra-packets <i>number</i>
Tree	in-matched-ra-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-octets *number*

Description	The total number of octets received in input packets, counting transit and terminating traffic
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-octets <i>number</i>
Tree	in-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-packets *number*

Description	The total number of input packets received, counting transit and terminating traffic
--------------------	--

This equals the sum of: in-error-packets in-discarded-packets (also includes IP/MPLS packets) in-terminated-packets (also includes IP/MPLS packets) in-forwarded-packets

Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-packets <i>number</i>
Tree	in-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-terminated-octets *number*

Description	The total number of octets in input IPv4 packets or IPv6 packets or both that were received on this subinterface and counted in in-terminated-packets
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-terminated-octets <i>number</i>
Tree	in-terminated-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

in-terminated-packets *number*

Description	The total number of input IPv4 packets or IPv6 packets or both 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: This also includes terminating IP/MPLS packets.
Context	interface name <i>string</i> subinterface index <i>number</i> statistics in-terminated-packets <i>number</i>
Tree	in-terminated-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-clear *string*

Description	Timestamp of the last time the subinterface counters were cleared.
Context	interface name <i>string</i> subinterface index <i>number</i> statistics last-clear <i>string</i>

Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

out-discarded-packets *number*

Description	The total number of IPv4 packets or IPv6 packets or both, originating and transit, sent towards this subinterface that were dropped. This also includes IP/MPLS packets dropped by egress interface ACL drop action.
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-discarded-packets <i>number</i>
Tree	out-discarded-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-error-packets *number*

Description	The number of IPv4 packets or IPv6 packets or both, 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. On 7250 IXR systems this is incremented when the IPv4 packet size exceeds the IP MTU and fragmentation was not allowed or not supported
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-error-packets <i>number</i>
Tree	out-error-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

out-forwarded-octets *number*

Description	The number of octets in transit IPv4 packets or IPv6 packets or both which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-forwarded-octets <i>number</i>
Tree	out-forwarded-octets

Default	0
Configurable	False
Platforms	Supported on all platforms

out-forwarded-packets *number*

Description	The number of transit IPv4 packets or IPv6 packets or both which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-forwarded-packets <i>number</i>
Tree	out-forwarded-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-octets *number*

Description	The total number of octets in IPv4 packets or IPv6 packets or both delivered to the lower layers for transmission
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-octets <i>number</i>
Tree	out-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-originated-octets *number*

Description	The number of octets in IPv4 packets or IPv6 packets or both which originated on the CPM and which the router attempted to route out this subinterface
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-originated-octets <i>number</i>
Tree	out-originated-octets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-originated-packets *number*

Description	The number of IPv4 packets or IPv6 packets or both which originated on the CPM and which the router attempted to route out this subinterface This includes all originated ICMP/ICMPv6 messages.
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-originated-packets <i>number</i>
Tree	out-originated-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-packets *number*

Description	The total number of IPv4 packets or IPv6 packets or both 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>
Context	interface name <i>string</i> subinterface index <i>number</i> statistics out-packets <i>number</i>
Tree	out-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

type *identityref*

Description	The value of this leaf indicates the context in which the ethernet subinterface will be used in
Context	interface name <i>string</i> subinterface index <i>number</i> type <i>identityref</i>
Tree	type
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 • local-mirror-dest indicates subinterface is used in a mirroring destination SPAN context
Configurable	True

Platforms Supported on all platforms

vlan

Description Parameters for VLAN definition under SRL interfaces.

Context [interface name](#) *string* [subinterface](#) *index* *number* [vlan](#)

Tree [vlan](#)

Configurable True

Platforms Supported on all platforms

encap

Description VLAN match parameters for the associated subinterface.

Context [interface name](#) *string* [subinterface](#) *index* *number* [vlan](#) [encap](#)

Tree [encap](#)

Configurable True

Platforms Supported on all platforms

single-tagged

Description When present, tagged frames with a specific, non-zero, outer VLAN ID are associated to the subinterface. (The outer VLAN-ID tag is considered service delimiting and it is stripped at ingress and restored/added on egress.).

Context [interface name](#) *string* [subinterface](#) *index* *number* [vlan](#) [encap](#) [single-tagged](#)

Tree [single-tagged](#)

Configurable True

Platforms Supported on all platforms

vlan-id (*number* | *keyword*)

Description VLAN identifier for single-tagged packets.

Context [interface name](#) *string* [subinterface](#) *index* *number* [vlan](#) [encap](#) [single-tagged](#) [vlan-id](#) (*number* | *keyword*)

Tree [vlan-id](#)

Range 1 to 4094

Options

- any

Configurable True

Platforms Supported on all platforms

untagged

Description When present, untagged frames and VLAN ID 0 priority tagged frames are associated to the subinterface when it belongs to an interface with vlan-tagging enabled.

Context [interface name](#) *string* [subinterface index](#) *number* [vlan encap untagged](#)

Tree [untagged](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

tpid *identityref*

Description Optionally set the tag protocol identifier field (TPID) that is accepted on the VLAN

Context [interface name](#) *string* [tpid identityref](#)

Tree [tpid](#)

Options

- [TPID_0X8100](#)
Default TPID value for 802.1q single-tagged VLANs.
- [TPID_0X88A8](#)
TPID value for 802.1ad provider bridging, QinQ or stacked VLANs.
- [TPID_0X9100](#)
Alternate TPID value.
- [TPID_0X9200](#)
Alternate TPID value.
- [TPID_ANY](#)
A wildcard that matches any of the generally used TPID values for singly- or multiply-tagged VLANs. Equivalent to matching any of [TPID_0X8100](#), [TPID_0X88A8](#), [TPID_0X9100](#) and [TPID_0x9200](#). This value is only applicable where the TPID of a packet is being matched.

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

traffic-rate

Description Container for traffic rate statistics

Context	interface name <i>string</i> traffic-rate
Tree	traffic-rate
Configurable	False
Platforms	Supported on all platforms

in-bps *number*

Description	The ingress bandwidth utilization of the port, updated every 10 seconds
Context	interface name <i>string</i> traffic-rate in-bps <i>number</i>
Tree	in-bps
Configurable	False
Platforms	Supported on all platforms

out-bps *number*

Description	The egress bandwidth utilization of the port, updated every 10 seconds
Context	interface name <i>string</i> traffic-rate out-bps <i>number</i>
Tree	out-bps
Configurable	False
Platforms	Supported on all platforms

transceiver

Description	Enter the transceiver context
Context	interface name <i>string</i> transceiver
Tree	transceiver
Configurable	True
Platforms	Supported on all platforms

channel [index](#) *number*

Description	List of physical channels supported by the transceiver that are associated with this particular port
Context	interface name <i>string</i> transceiver channel index <i>number</i>
Tree	channel
Configurable	False
Platforms	Supported on all platforms

index number

Description	Index of the physical channel or lane
Context	interface name <i>string</i> transceiver channel index number
Range	1 to 10
Configurable	False
Platforms	Supported on all platforms

input-power

Description	Enter the input-power context
Context	interface name <i>string</i> transceiver channel index number input-power
Tree	input-power
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index number input-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver channel index number input-power high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current value of the optical Rx power in dBm
Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False
Platforms	Supported on all platforms

low-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Configurable	False
Platforms	Supported on all platforms

low-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> input-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

laser-bias-current

Description	Enter the laser-bias-current context
Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current
Tree	laser-bias-current
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
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
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
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
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current value of the laser bias current in mA
Context	interface name <i>string</i> transceiver channel index <i>number</i> laser-bias-current latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False
Platforms	Supported on all platforms

low-alarm-condition *boolean*

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
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
Configurable	False
Platforms	Supported on all platforms

low-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
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
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

output-power

Description	Enter the output-power context
Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power
Tree	output-power
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current value of the optical Tx power in dBm
Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False
Platforms	Supported on all platforms

low-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Configurable	False
Platforms	Supported on all platforms

low-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver channel index <i>number</i> output-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *decimal-number*

Description	Read from the installed transceiver
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
Configurable	False
Platforms	Supported on all platforms

wavelength *decimal-number*

Description	Wavelength of the transmitting laser in nanometers
Context	interface name <i>string</i> transceiver channel index <i>number</i> wavelength <i>decimal-number</i>
Tree	wavelength
Configurable	False
Platforms	Supported on all platforms

connector-type *keyword*

Description	Specifies the fiber connector type of the transceiver associated with the port.
Context	interface name <i>string</i> transceiver connector-type <i>keyword</i>
Tree	connector-type
Options	<ul style="list-style-type: none"> • SC • FC-STYLE1-COPPER • FC-STYLE2-COPPER • BNC-OR-TNC • FC-COAX • FIBER-JACK • LC • MT-RJ • MU • SG • OPTICAL-PIGTAIL • MPO-1x12 • MPO-2x16 • HSSDC • COPPER-PIGTAIL • RJ45 • no-separable-connector • MXC-2x16 • CS-OPTICAL-CONNECTOR • SN-OPTICAL-CONNECTOR • MPO-2x12 • MPO-1x16 • unknown
Configurable	False
Platforms	Supported on all platforms

date-code *string*

Description	Transceiver date code.
Context	interface name <i>string</i> transceiver date-code <i>string</i>
Tree	date-code
Configurable	False

Platforms Supported on all platforms

ddm-events *boolean*

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.
When read from state this leaf always returns false (even if the configured value is true) when the Ethernet port is a copper/RJ45 port.

Context [interface name](#) *string* [transceiver](#) [ddm-events](#) *boolean*

Tree [ddm-events](#)

Configurable True

Platforms Supported on all platforms

ethernet-pmd *string*

Description Specifies the Ethernet compliance code of the transceiver associated with the port.

Context [interface name](#) *string* [transceiver](#) [ethernet-pmd](#) *string*

Tree [ethernet-pmd](#)

Configurable False

Platforms Supported on all platforms

fault-condition *boolean*

Description Indicates if a fault condition exists in the transceiver.

Context [interface name](#) *string* [transceiver](#) [fault-condition](#) *boolean*

Tree [fault-condition](#)

Configurable False

Platforms Supported on all platforms

form-factor *keyword*

Description Specifies the transceiver form factor associated with the port.

Context [interface name](#) *string* [transceiver](#) [form-factor](#) *keyword*

Tree [form-factor](#)

Options	<ul style="list-style-type: none"> • CFP2 • CFP2-ACO • CFP4 • QSFP • QSFPplus • QSFP28 • QSFPDD • SFP • SFPplus • Non-pluggable • Other • SFP28
Configurable	False
Platforms	Supported on all platforms

forward-error-correction *keyword*

Description	<p>The forward error correction algorithm to use on the optical channel. The same FEC algorithm must be used at both ends of a link.</p> <p>25G interfaces support disabled, base-r rs-108 and rs-528; configuring other (incompatible) options will bring the port down. The FEC requirement for a 25G interface depends on the cable type. A CA-N DAC cable has a loss specification that requires no FEC. A CA-S DAC cable requires base-r FEC at a minimum. A CA-L DAC cable requires the stronger rs-108 Reed Solomon FEC.</p> <p>100G interfaces support disabled and rs-528; configuring other (incompatible) options will bring the port down.</p> <p>400G interfaces require rs-544; configuring other (unsupported) options will bring the port down.</p>
Context	<code>interface name string transceiver forward-error-correction keyword</code>
Tree	<code>forward-error-correction</code>
Options	<ul style="list-style-type: none"> • disabled • rs-528 • rs-544 • base-r <ul style="list-style-type: none"> BASE-R FEC algorithm for 25GbE interfaces (also known as fire-code). • rs-108 <ul style="list-style-type: none"> Reed Solomon FEC algorithm for 25GbE interfaces.

Configurable	True
Platforms	Supported on all platforms

input-power

Description	Enter the input-power context
Context	interface name <i>string</i> transceiver input-power
Tree	input-power
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver input-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver input-power high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver input-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver input-power high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current value of the optical Rx power in dBm
Context	interface name <i>string</i> transceiver input-power latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False
Platforms	Supported on all platforms

low-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver input-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Configurable	False
Platforms	Supported on all platforms

low-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver input-power low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver input-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver input-power low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Configurable	False
Platforms	Supported on all platforms

laser-bias-current

Description	Enter the laser-bias-current context
Context	interface name <i>string</i> transceiver laser-bias-current
Tree	laser-bias-current
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver laser-bias-current high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver laser-bias-current high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver laser-bias-current high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver laser-bias-current high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current value of the laser bias current in mA
Context	interface name <i>string</i> transceiver laser-bias-current latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False
Platforms	Supported on all platforms

low-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver laser-bias-current low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Configurable	False
Platforms	Supported on all platforms

low-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver laser-bias-current low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver laser-bias-current low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver laser-bias-current low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Configurable	False
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The reason for the transceiver being operationally down.
Context	interface name <i>string</i> transceiver oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • not-present • read-failure • checksum-failure • unknown-transceiver • tx-laser-disabled • unsupported-breakout • port-disabled • connector-transceiver-down
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	<p>The operational state of the transceiver.</p> <p>The oper-state is always down when the Ethernet port is a copper/RJ45 port.</p>
Context	interface name <i>string</i> transceiver oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up • down
Configurable	False
Platforms	Supported on all platforms

output-power

Description	Enter the output-power context
Context	interface name <i>string</i> transceiver output-power
Tree	output-power
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver output-power high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver output-power high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver output-power high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver output-power high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current value of the optical Tx power in dBm
Context	interface name <i>string</i> transceiver output-power latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False
Platforms	Supported on all platforms

low-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver output-power low-alarm-condition <i>boolean</i>
Tree	low-alarm-condition
Configurable	False
Platforms	Supported on all platforms

low-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver output-power low-alarm-threshold <i>decimal-number</i>
Tree	low-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver output-power low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *decimal-number*

Description	Read from the installed transceiver
--------------------	-------------------------------------

Context	interface name <i>string</i> transceiver output-power low-warning-threshold <i>decimal-number</i>
Tree	low-warning-threshold
Configurable	False
Platforms	Supported on all platforms

serial-number *string*

Description	Transceiver serial number.
Context	interface name <i>string</i> transceiver serial-number <i>string</i>
Tree	serial-number
Configurable	False
Platforms	Supported on all platforms

temperature

Description	Enter the temperature context
Context	interface name <i>string</i> transceiver temperature
Tree	temperature
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition *boolean*

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
Context	interface name <i>string</i> transceiver temperature high-alarm-condition <i>boolean</i>
Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver temperature high-alarm-threshold <i>number</i>
Tree	high-alarm-threshold
Configurable	False

Platforms Supported on all platforms

high-warning-condition *boolean*

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

Context [interface name](#) *string* [transceiver temperature high-warning-condition](#) *boolean*

Tree [high-warning-condition](#)

Configurable False

Platforms Supported on all platforms

high-warning-threshold *number*

Description Read from the installed transceiver

Context [interface name](#) *string* [transceiver temperature high-warning-threshold](#) *number*

Tree [high-warning-threshold](#)

Configurable False

Platforms Supported on all platforms

latest-value *number*

Description The current temperature of the transceiver module in degrees Celsius

Context [interface name](#) *string* [transceiver temperature latest-value](#) *number*

Tree [latest-value](#)

Configurable False

Platforms Supported on all platforms

low-alarm-condition *boolean*

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

Context [interface name](#) *string* [transceiver temperature low-alarm-condition](#) *boolean*

Tree [low-alarm-condition](#)

Configurable False

Platforms Supported on all platforms

low-alarm-threshold *number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver temperature low-alarm-threshold <i>number</i>
Tree	low-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

low-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver temperature low-warning-condition <i>boolean</i>
Tree	low-warning-condition
Configurable	False
Platforms	Supported on all platforms

low-warning-threshold *number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver temperature low-warning-threshold <i>number</i>
Tree	low-warning-threshold
Configurable	False
Platforms	Supported on all platforms

tx-laser *boolean*

Description	Enable (true) or disable (false) the transmit laser of the transceiver. When read from state this leaf always returns false (even if the configured value is true) when the Ethernet port is a copper/RJ45 port. Default is true (for interfaces that support transceivers).
Context	interface name <i>string</i> transceiver tx-laser <i>boolean</i>
Tree	tx-laser
Configurable	True
Platforms	Supported on all platforms

vendor string

Description	Name of the transceiver vendor.
Context	interface name string transceiver vendor string
Tree	vendor
Configurable	False
Platforms	Supported on all platforms

vendor-part-number string

Description	Vendor's part number for the transceiver.
Context	interface name string transceiver vendor-part-number string
Tree	vendor-part-number
Configurable	False
Platforms	Supported on all platforms

vendor-revision string

Description	Vendor's revision number for the transceiver.
Context	interface name string transceiver vendor-revision string
Tree	vendor-revision
Configurable	False
Platforms	Supported on all platforms

voltage

Description	Enter the voltage context
Context	interface name string transceiver voltage
Tree	voltage
Configurable	False
Platforms	Supported on all platforms

high-alarm-condition boolean

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
Context	interface name string transceiver voltage high-alarm-condition boolean

Tree	high-alarm-condition
Configurable	False
Platforms	Supported on all platforms

high-alarm-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver voltage high-alarm-threshold <i>decimal-number</i>
Tree	high-alarm-threshold
Configurable	False
Platforms	Supported on all platforms

high-warning-condition *boolean*

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
Context	interface name <i>string</i> transceiver voltage high-warning-condition <i>boolean</i>
Tree	high-warning-condition
Configurable	False
Platforms	Supported on all platforms

high-warning-threshold *decimal-number*

Description	Read from the installed transceiver
Context	interface name <i>string</i> transceiver voltage high-warning-threshold <i>decimal-number</i>
Tree	high-warning-threshold
Configurable	False
Platforms	Supported on all platforms

latest-value *decimal-number*

Description	The current voltage reading of the transceiver module (in Volts)
Context	interface name <i>string</i> transceiver voltage latest-value <i>decimal-number</i>
Tree	latest-value
Configurable	False

Platforms Supported on all platforms

low-alarm-condition *boolean*

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

Context [interface name](#) *string* [transceiver voltage](#) [low-alarm-condition](#) *boolean*

Tree [low-alarm-condition](#)

Configurable False

Platforms Supported on all platforms

low-alarm-threshold *decimal-number*

Description Read from the installed transceiver

Context [interface name](#) *string* [transceiver voltage](#) [low-alarm-threshold](#) *decimal-number*

Tree [low-alarm-threshold](#)

Configurable False

Platforms Supported on all platforms

low-warning-condition *boolean*

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

Context [interface name](#) *string* [transceiver voltage](#) [low-warning-condition](#) *boolean*

Tree [low-warning-condition](#)

Configurable False

Platforms Supported on all platforms

low-warning-threshold *decimal-number*

Description Read from the installed transceiver

Context [interface name](#) *string* [transceiver voltage](#) [low-warning-threshold](#) *decimal-number*

Tree [low-warning-threshold](#)

Configurable False

Platforms Supported on all platforms

wavelength *decimal-number*

Description Wavelength of the transmitting laser in nanometers

Context [interface name](#) *string* [transceiver](#) [wavelength](#) *decimal-number*

Tree [wavelength](#)

Configurable False

Platforms Supported on all platforms

vlan-tagging *boolean*

Description When set to true the interface is allowed to accept frames with one or more VLAN tags

Context [interface name](#) *string* [vlan-tagging](#) *boolean*

Tree [vlan-tagging](#)

Configurable True

Platforms Supported on all platforms

6 network-instance

```

network-instance name string
+ admin-state keyword
+ 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-with-zone)
      - origin keyword
      - originator-id (ipv4-address | ipv6-address)
      - pmsi-tunnel
        - flags
          - assisted-replication-type keyword
          - leaf-information-required boolean
          - pruned-flood-list
            - broadcast-multicast keyword
            - unknown-unicast keyword
          - tunnel-endpoint (ipv4-address | ipv6-address)
          - tunnel-type keyword
          - vni number
      - unknown-attributes
        - unknown-attribute unknown-attr-index number
          - attr-len number
          - attr-type number
          - extended boolean
          - optional boolean
          - partial boolean
          - transitive boolean
  - evpn
    - rib-in-out
      - rib-in-post

```

```

- ethernet-ad-routes route-distinguisher (string | string | string |
string) esi string ethernet-tag-id number neighbor (ipv4-address | ipv6-address)
  - attr-id reference
  - best-route boolean
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean
    - rejected-route boolean
  - last-modified string
  - neighbor-as number
  - pending-delete boolean
  - stale-route boolean
  - tie-break-reason keyword
  - used-route boolean
  - valid-route boolean
  - vni number
- ethernet-segment-routes route-distinguisher (string | string | string |
string) esi string originating-router (ipv4-address | ipv6-address) neighbor (ipv4-address |
ipv6-address)
  - attr-id reference
  - best-route boolean
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean
    - rejected-route boolean
  - last-modified string
  - neighbor-as number
  - pending-delete boolean
  - stale-route boolean
  - tie-break-reason keyword
  - used-route boolean
  - valid-route boolean
- imet-routes route-distinguisher (string | string | string | string) originating-
router (ipv4-address | ipv6-address) ethernet-tag-id number neighbor (ipv4-address | ipv6-
address)
  - attr-id reference
  - best-route boolean
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean
    - rejected-route boolean
  - last-modified string
  - neighbor-as number
  - pending-delete boolean
  - stale-route boolean
  - tie-break-reason keyword
  - used-route boolean
  - valid-route boolean
- ip-prefix-routes route-distinguisher (string | string | string |
string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix | ipv6-
prefix) neighbor (ipv4-address | ipv6-address)
  - attr-id reference
  - best-route boolean
  - esi string
  - gateway-ip (ipv4-address | ipv6-address)
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean

```

```

- rejected-route boolean
- last-modified string
- neighbor-as number
- pending-delete boolean
- stale-route boolean
- tie-break-reason keyword
- used-route boolean
- valid-route boolean
- vni number
- mac-ip-routes route-distinguisher (string | string | string | string) mac-length number mac-address string ip-address (ipv4-address | ipv6-address) ethernet-tag-id number neighbor (ipv4-address | ipv6-address)
  - attr-id reference
  - best-route boolean
  - esi string
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean
    - rejected-route boolean
  - last-modified string
  - neighbor-as number
  - pending-delete boolean
  - stale-route boolean
  - tie-break-reason keyword
  - used-route boolean
  - valid-route boolean
  - vni number
- rib-in-pre
  - ethernet-ad-routes route-distinguisher (string | string | string | string) esi string ethernet-tag-id number neighbor (ipv4-address | ipv6-address)
    - attr-id reference
    - vni number
  - ethernet-segment-routes route-distinguisher (string | string | string | string) esi string originating-router (ipv4-address | ipv6-address) neighbor (ipv4-address | ipv6-address)
    - attr-id reference
    - imet-routes route-distinguisher (string | string | string | string) originating-router (ipv4-address | ipv6-address) ethernet-tag-id number neighbor (ipv4-address | ipv6-address)
      - attr-id reference
      - ip-prefix-routes route-distinguisher (string | string | string | string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix | ipv6-prefix) neighbor (ipv4-address | ipv6-address)
        - attr-id reference
        - esi string
        - gateway-ip (ipv4-address | ipv6-address)
        - vni number
      - mac-ip-routes route-distinguisher (string | string | string | string) mac-length number mac-address string ip-address (ipv4-address | ipv6-address) ethernet-tag-id number neighbor (ipv4-address | ipv6-address)
        - attr-id reference
        - esi string
        - vni number
    - rib-out-post
      - ethernet-ad-routes route-distinguisher (string | string | string | string) esi string ethernet-tag-id number neighbor (ipv4-address | ipv6-address)
        - attr-id reference
        - next-hop (ipv4-address | ipv6-address)
        - vni number
      - ethernet-segment-routes route-distinguisher (string | string | string | string) esi string originating-router (ipv4-address | ipv6-address) neighbor (ipv4-address | ipv6-address)
        - attr-id reference
        - next-hop (ipv4-address | ipv6-address)

```

```

- imet-routes route-distinguisher (string | string | string | string) originating-
router (ipv4-address | ipv6-address) ethernet-tag-id number neighbor (ipv4-address | ipv6-
address)
  - attr-id reference
  - next-hop (ipv4-address | ipv6-address)
  - ip-prefix-routes route-distinguisher (string | string | string |
string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix | ipv6-
prefix) neighbor (ipv4-address | ipv6-address)
    - attr-id reference
    - esi string
    - gateway-ip (ipv4-address | ipv6-address)
    - next-hop (ipv4-address | ipv6-address)
    - vni number
  - mac-ip-routes route-distinguisher (string | string | string | string) mac-
length number mac-address string ip-address (ipv4-address | ipv6-address) ethernet-tag-
id number neighbor (ipv4-address | ipv6-address)
    - attr-id reference
    - esi string
    - next-hop (ipv4-address | ipv6-address)
    - vni number
- ipv4-unicast
- local-rib
  - routes prefix (ipv4-prefix | ipv6-prefix) neighbor (ipv4-address | ipv6-address-
with-zone) origin-protocol identityref
    - attr-id reference
    - best-route boolean
    - group-best boolean
    - invalid-reason
      - as-loop boolean
      - cluster-loop boolean
      - next-hop-unresolved boolean
      - rejected-route boolean
    - last-modified string
    - neighbor-as number
    - 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-
with-zone)
      - attr-id reference
      - best-route boolean
      - group-best boolean
      - invalid-reason
        - as-loop boolean
        - cluster-loop boolean
        - next-hop-unresolved boolean
        - rejected-route boolean
      - last-modified string
      - neighbor-as number
      - 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-
with-zone)
        - attr-id reference
    - rib-out-post
      - routes prefix (ipv4-prefix | ipv6-prefix) neighbor (ipv4-address | ipv6-address-
with-zone)
        - attr-id reference

```

```

- ipv6-unicast
- local-rib
  - routes prefix (ipv4-prefix | ipv6-prefix) neighbor (ipv4-address | ipv6-address-
with-zone) origin-protocol identityref
  - attr-id reference
  - best-route boolean
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean
    - rejected-route boolean
  - last-modified string
  - neighbor-as number
  - 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-
with-zone)
  - attr-id reference
  - best-route boolean
  - group-best boolean
  - invalid-reason
    - as-loop boolean
    - cluster-loop boolean
    - next-hop-unresolved boolean
    - rejected-route boolean
  - last-modified string
  - neighbor-as number
  - pending-delete boolean
  - stale-route boolean
  - tie-break-reason keyword
  - used-route boolean
  - valid-route boolean
- rib-in-pre
with-zone)
  - attr-id reference
- rib-out-post
with-zone)
  - routes prefix (ipv4-prefix | ipv6-prefix) neighbor (ipv4-address | ipv6-address-
with-zone)
  - 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 (keyword | number)
+ hold-down-time (keyword | 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
    - is-protected boolean
    - last-update string
    - not-programmed-reason keyword
    - type keyword
+ protect-anycast-gw-mac boolean
- reserved-macs
  - mac address string
    - users application string
+ static-mac
+ mac address string
  + destination (keyword | reference)
- statistics
  - active-entries number
  - failed-entries number
  - mac-type type keyword
    - active-entries number
    - failed-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-error-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-error-packets number
      - out-packets number
+ interface name string
  - index number
  - mac-relearn-only boolean
  - multicast-forwarding keyword
  - oper-down-reason keyword

```

```

- oper-mac-learning keyword
- oper-mac-learning-disabled-reason keyword
- oper-state keyword
+ ip-forwarding
+ last-resort-lookup
+ network-instance reference
+ 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
+ icmp-tunneling boolean
+ static-entry top-label number preference number
+ admin-state keyword
+ collect-stats boolean
- installed boolean
+ next-hop-group reference
+ operation keyword
- resolved-next-hop-group-id reference
+ mpls-forwarding
+ forward-received-packets 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
+ failure-detection
+ enable-bfd
+ local-address (ipv4-address | ipv6-address)
+ local-discriminator number
+ remote-discriminator number
+ ip-address (ipv4-address | ipv6-address)
+ pushed-mpls-label-stack (number | keyword)
+ resolve boolean
- oper-mac-vrf-mtu number
- oper-state keyword
+ policy-forwarding
+ interface subinterface reference
+ apply-forwarding-policy reference
+ policy policy-id string
+ description string
+ rule sequence-id number
+ action
+ network-instance reference
+ description string
+ match
+ ipv4
+ dscp-set (number | keyword)
+ protocol (number | keyword)
+ source-ip
+ prefix string
- tcam-entries number
- tcam-entries number
+ 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)
      + allowed-peer-as string
      + peer-group reference
    + max-sessions number
  + interface interface-name reference
    + allowed-peer-as string
    + peer-group reference
+ ebgp-default-policy
  + export-reject-all boolean
  + import-reject-all boolean
+ evpn
  - active-routes number
  + admin-state keyword
  + advertise-ipv6-next-hops boolean
  + inter-as-vpn boolean
  + keep-all-routes boolean
  + rapid-update boolean
  - received-routes number
+ 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
  + evpn
    + admin-state keyword
    + advertise-ipv6-next-hops boolean
    + prefix-limit
      + max-received-routes number
      + warning-threshold-pct number
  + 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
+ multihop
+ admin-state keyword
+ maximum-hops number
+ 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 | string)
+ 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
+ next-hop-resolution
+ ipv4-next-hops
  + tunnel-resolution
    + allowed-tunnel-types identityref
    + mode keyword
+ 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
+ next-hop-resolution
+ ipv4-next-hops
  + tunnel-resolution
    + allowed-tunnel-types identityref
    + mode keyword
- received-routes number
+ local-preference number
- maintenance-group string
+ neighbor peer-address (ipv4-address | ipv6-address-with-zone)
+ 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
- transmit-active boolean
+ description string
- discovered-by-lldp boolean
- dynamic-neighbor boolean
- established-transitions number
+ evpn
- active-routes number
+ admin-state keyword
+ advertise-ipv6-next-hops boolean
- oper-state keyword
+ prefix-limit
  + max-received-routes number
  + warning-threshold-pct number
- received-routes number
- rejected-routes number
- sent-routes 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-state keyword
+ local-as as-number number
+ prepend-global-as boolean
+ prepend-local-as boolean
+ local-preference number
- maintenance-group string
+ multihop
+ admin-state keyword
+ maximum-hops number
+ next-hop-self boolean
+ peer-as number
+ peer-group reference
- peer-router-id string
- peer-type keyword
- received-afi-safi keyword
- received-capabilities keyword
- received-end-of-rib keyword
- received-messages
  - last-notification-error-code keyword
  - last-notification-error-subcode keyword
  - last-notification-time string
  - last-update-time string
  - malformed-updates number
  - queue-depth number
  - route-refresh number
  - total-messages number
  - total-non-updates number
  - total-notifications 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
- last-notification-error-code keyword
- last-notification-error-subcode keyword
- last-notification-time string
- queue-depth number
- route-refresh number
- total-messages number
- total-non-updates number
- total-notifications 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 | string)
- 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 (ipv4-address | ipv6-address)
+ 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
+   single-hop-connected-check boolean
+   tcp-mss number
-   under-maintenance boolean
+ bgp-evpn
+   bgp-instance id reference
+   admin-state keyword
+   default-admin-tag number
+   ecmp number
+   encapsulation-type keyword
+   evi number
+   ingress-replication-bum-label boolean
-   oper-down-reason keyword
-   oper-state keyword
+   routes
+     bridge-table
+       inclusive-mcast
+       advertise boolean
+       originating-ip (ipv4-address | ipv6-address)
+       mac-ip
+       advertise boolean
+       advertise-arp-nd-only-with-mac-table-entry boolean
+       next-hop (keyword | ipv4-address | ipv6-address)
+       vlan-aware-bundle-eth-tag number
+     route-table
+     mac-ip
+     advertise-gateway-mac boolean
+   vxlan-interface reference
+ bgp-vpn
+   bgp-instance id number
+   export-policy reference
+   import-policy reference
-   oper-down-reason keyword
+   route-distinguisher
+   rd (string | string | string | string)
-   route-distinguisher-origin keyword
+   route-target
-   export-route-target-origin keyword
+   export-rt (string | string | string)
| string | string)
-   import-route-target-origin keyword
+   import-rt (string | string | string)
| string | string)
+   gribi
+   admin-state keyword
+   default-metric number
+   default-preference number
+   max-ecmp-hash-buckets-per-next-hop-group number
+   maximum-routes number
+   igmp
+   admin-state keyword
+   interface interface-name reference
+   admin-state keyword
-   counters
-   error
-   bad-encoding
-   bad-length
-   import-policy-drops
-   local-scope
-   missing-router-alert
-   non-local
-   out-of-memory-drops
-   reached-maximum-number-group-sources
-   reached-maximum-number-groups
-   reached-maximum-number-sources
-   reserved-scope

```

```

- unknown-type
- wrong-version
- received
- drops
- general-queries
- group-queries
- group-source-queries
- leaves
- v1-reports
- v2-reports
- v3-reports
- transmitted
- errors
- general-queries
- group-queries
- group-source-queries
- group-count number
+ import-policy reference
+ max-group-sources number
+ max-groups number
+ max-sources number
- membership-groups
- group group string
- expiry-time number
- filter-mode keyword
- group-type keyword
- igmp-compatibility-mode keyword
- last-reporter (ipv4-address | ipv6-address)
- source source string
- expiry-time number
- forwarding-state keyword
- source-type keyword
- up-time number
- up-time number
- v1-host-timer number
- v2-host-timer number
- oper-state keyword
- oper-version number
- querier
- address string
- expiry-time number
- up-time number
+ query-interval number
+ query-last-member-interval number
+ query-response-interval number
+ router-alert-check boolean
+ ssm
+ mappings
+ group-range start string end string
+ source source string
+ static
+ group-range start string end string
+ source source string
+ starg
+ subnet-check boolean
+ version number
- oper-state keyword
+ query-interval number
+ query-last-member-interval number
+ query-response-interval number
+ robust-count number
+ ssm
+ mappings
+ group-range start string end string
+ source source string
+ trace-options

```

```

+ trace
+ interface
+   all
+   name reference
+ packet
+   interface
+   all
+   name reference
+   modifier keyword
+   type keyword
+ isis
+ instance name string
+ admin-state keyword
+ attached-bit
+ ignore boolean
+ suppress boolean
+ authentication
+   csnp-authentication
+   check-received keyword
+   generate boolean
+   hello-authentication
+   check-received keyword
+   generate boolean
+   key
+   auth-password string
+   crypto-algorithm keyword
+   keychain reference
+   lsp-authentication
+   check-received keyword
+   generate boolean
+   psnp-authentication
+   check-received keyword
+   generate boolean
+ auto-cost
+ reference-bandwidth number
+ export-policy reference
+ graceful-restart
+ helper-mode boolean
- hostnames
- system-id host-system-id string
- hostname string
+ 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
+ check-received keyword

```

```

    + generate boolean
    + key
      + auth-password string
      + crypto-algorithm keyword
    + 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
  + ldp-synchronization
    + disable
      - duration number
    + end-of-lib boolean
    + hold-down-timer number
      - sync-state keyword
  + level level-number number
    + authentication
      + hello-authentication
        + check-received keyword
        + generate boolean
      + key
        + auth-password string
        + crypto-algorithm keyword
      + keychain reference
    + disable boolean
    + ipv6-unicast-metric number
    + metric number
    + priority number
    + timers
      + hello-interval number
      + hello-multiplier number
  - oper-state keyword
  + passive boolean
  + segment-routing
    + mpls
      + ipv4-node-sid
        + index number
      + ipv6-node-sid
        + index number
  + 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
  + ldp-synchronization
    + end-of-lib boolean
    + hold-down-timer number
  + level level-number number
    + authentication
      + csnp-authentication
        + check-received keyword
        + generate boolean
      + hello-authentication
        + check-received keyword

```

```

+ generate boolean
+ key
+ auth-password string
+ crypto-algorithm keyword
+ keychain reference
+ lsp-authentication
+ check-received keyword
+ generate boolean
+ psnp-authentication
+ check-received keyword
+ generate 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
- sub-tlvs
- route-tag-32bit number
- route-tag-64bit number
- segment-routing-prefix-sid
- algorithm keyword
- explicit-null boolean
- local boolean
- node-sid boolean
- penultimate-hop-popping boolean
- re-advertised boolean
- sr-index-or-label number
- value boolean
- extended-is-reachability neighbor string
- default-metric number
- sub-tlvs
- ipv4-interface-address string
- ipv4-neighbor-address string
- ipv6-interface-address string
- ipv6-neighbor-address string
- link-msd
- msd-info msd-type (keyword | number) msd-value number
- segment-routing-adjacency-sid sr-index-or-label number
- adj-set boolean
- backup boolean
- ipv6-family boolean
- local boolean
- persistent boolean
- value boolean
- weight number
- segment-routing-lan-adjacency-sid sr-index-or-label number
- adj-set boolean
- backup boolean
- ipv6-family boolean

```

```

- local boolean
- neighbor-system-id string
- persistent boolean
- value boolean
- weight number
- 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
- sub-tlvs
- route-tag-32bit number
- route-tag-64bit number
- segment-routing-prefix-sid
- algorithm keyword
- explicit-null boolean
- local boolean
- node-sid boolean
- penultimate-hop-popping boolean
- re-advertised boolean
- sr-index-or-label number
- value boolean
- is-reachability neighbor string
- default-metric number
- default-metric-type keyword
- mt-ipv4-reachability ipv4-prefix string
- down boolean
- metric number
- mt-id number
- sub-tlvs
- route-tag-32bit number
- route-tag-64bit number
- segment-routing-prefix-sid
- algorithm keyword
- explicit-null boolean
- local boolean
- node-sid boolean
- penultimate-hop-popping boolean
- re-advertised boolean
- sr-index-or-label number
- value boolean
- mt-ipv6-reachability ipv6-prefix string
- down boolean
- external boolean
- metric number
- mt-id number
- sub-tlvs
- route-tag-32bit number
- route-tag-64bit number
- segment-routing-prefix-sid
- algorithm keyword
- explicit-null boolean
- local boolean
- node-sid boolean
- penultimate-hop-popping boolean
- re-advertised boolean

```

```

    - sr-index-or-label number
    - value boolean
- mt-is-reachability-neighbor string
- default-metric number
- mt-id number
- sub-tlvs
  - ipv4-interface-address string
  - ipv4-neighbor-address string
  - ipv6-interface-address string
  - ipv6-neighbor-address string
  - link-msd
    - msd-info msd-type (keyword | number) msd-value number
  - segment-routing-adjacency-sid sr-index-or-label number
    - adj-set boolean
    - backup boolean
    - ipv6-family boolean
    - local boolean
    - persistent boolean
    - value boolean
    - weight number
  - segment-routing-lan-adjacency-sid sr-index-or-label number
    - adj-set boolean
    - backup boolean
    - ipv6-family boolean
    - local boolean
    - neighbor-system-id string
    - persistent boolean
    - value boolean
    - weight number
- multi-topology
  - topology mt-id number
  - attached boolean
  - overload boolean
- nlpid keyword
- purge-oi string
- router-capability
  - leaked-down boolean
  - router-id string
  - scope-is-domain-wide boolean
  - sub-tlvs
    - node-msd
      - msd-info msd-type (keyword | number) msd-value number
    - sr-algorithm
      - algorithm number
    - sr-capabilities
      - ipv4-support boolean
      - ipv6-support boolean
      - srgb-descriptor sr-index-or-label number range number
    - sr-local-block
      - srlb-descriptor sr-index-or-label number range number
  - te-router-id 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-area-id string
- oper-state keyword
- oper-system-id string
+ overload

```

```

+ advertise-external boolean
+ advertise-interlevel boolean
+ immediate
+ max-metric boolean
+ set-bit boolean
- instance-is-in-overload boolean
+ on-boot
+ max-metric boolean
+ set-bit boolean
+ timeout number
+ poi-tlv boolean
- restarting-neighbor-list
- neighbor system-id string
- hostname string
+ segment-routing
+ mpls
- sid-database
- prefix-sid prefix (ipv4-prefix | ipv6-prefix) sid-label-
value number multi-topology-id number algorithm number
- active boolean
- prefix-conflict boolean
- sid-conflict boolean
- sid-out-of-range boolean
- source-router system-id string level-number number
- flags
- explicit-null boolean
- local boolean
- node-sid boolean
- penultimate-hop-popping boolean
- re-advertised boolean
- local-system boolean
- statistics
- last-partial-spf string
- last-spf string
- partial-spf-runs number
- pdu pdu-name keyword
- dropped number
- processed number
- received 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
+ ldp
+ admin-state keyword
+ discovery
+ interfaces
+ hello-holdtime number
+ hello-interval number
+ interface name reference
+ hello-holdtime number

```

```

+ hello-interval number
+ ipv4
+ admin-state keyword
- hello-adjacencies
- adjacency lsr-id reference label-space-id reference
- hello-holdtime
- negotiated number
- neighbor-proposed number
- remaining number
- hello-received number
- hello-sent number
- local-address string
- remote-address string
- last-oper-state-change string
- oper-down-reason keyword
- oper-state keyword
- statistics
- hello-message-errors
- bad-message-length number
- bad-pdu-length number
- bad-protocol-version number
- malformed-tlv-value number
- hello-received number
- hello-sent number
+ trace-options
+ trace keyword
+ trace-options
+ trace keyword
+ graceful-restart
+ helper-enable boolean
+ max-reconnect-time number
+ max-recovery-time number
+ ipv4
- bindings
- advertised-address
- peer lsr-id reference label-space-id reference
- ip-address string
- advertised-prefix-fecs fec string lsr-id reference label-space-id reference
- egress-lsr-fec boolean
- label (number | keyword)
- label-status keyword
- label-type keyword
- received-address
- peer lsr-id reference label-space-id reference
- ip-address string
- received-prefix-fecs fec string lsr-id reference label-space-id reference
- ingress-lsr-fec boolean
- label (number | keyword)
- next-hop index number
- interface string
- next-hop (ipv4-address | ipv6-address)
- not-used-reason keyword
- used-in-forwarding boolean
+ fec-resolution
+ longest-prefix boolean
- last-oper-state-change string
- oper-down-reason keyword
- oper-state keyword
- oper-up-to-down-transitions number
- lsr-id string
+ multipath
+ max-paths number
+ peers
+ peer lsr-id string label-space-id number
- end-of-lib
- ipv4-prefix-fecs

```

```

- received boolean
- sent boolean
+ fec-limit number
- fec-limit-exceeded boolean
- graceful-restart
- peer-reconnect-time number
- peer-recovery-time number
- peer-restarting boolean
- Label-advertisement-mode
- negotiated keyword
- last-oper-state-change string
- overload
- local-router-is-overloaded boolean
- peer-is-overloaded boolean
- received-capabilities
- dual-stack-capability boolean
- dynamic-capability boolean
- entropy-label-capability boolean
- graceful-restart-capability boolean
- make-before-break-capability boolean
- multipoint-to-multipoint-capability boolean
- nokia-vendor-overload-capability boolean
- point-to-multipoint-capability boolean
- state-advertisement-control
- ipv4-prefix-disable boolean
- ipv6-prefix-disable boolean
- p2p-pseudowire-fec-128-disable boolean
- p2p-pseudowire-fec-129-disable boolean
- unrecognized-notification-capability boolean
- session-holdtime
- negotiated number
- peer-proposed number
- remaining number
- session-state keyword
- statistics
- address-statistics
- ipv4
- advertised-addresses number
- received-addresses number
- fec-statistics
- ipv4-prefix
- advertised-fecs number
- received-fecs number
- received-messages
- address number
- address-withdraw number
- capability number
- initialization number
- keepalive number
- label-abort-request number
- label-mapping number
- label-release number
- label-request number
- label-withdraw number
- notification number
- total-messages number
- sent-messages
- address number
- address-withdraw number
- capability number
- initialization number
- keepalive number
- label-abort-request number
- label-mapping number
- label-release number
- label-request number

```

```

    - label-withdraw number
    - notification number
    - total-messages number
+ tcp-transport
  - local-address string
  - local-port number
  - remote-address string
  - remote-port number
+ trace-options
  + trace keyword
+ session-keepalive-holdtime number
+ session-keepalive-interval number
+ trace-options
  + trace keyword
- statistics
  - fec-statistics
    - ipv4-prefix
      - advertised-fecs number
      - received-fecs number
    - protocol-errors
      - bad-ldp-identifier number
      - bad-message-length number
      - bad-pdu-length number
      - bad-protocol-version number
      - bad-tlv-length number
      - malformed-tlv-value number
      - missing-message-parameters number
      - session-rejected-bad-keepalive-time number
      - session-rejected-no-hello number
      - session-rejected-parameters-adv-mode number
      - session-rejected-parameters-label-range number
      - session-rejected-parameters-max-pdu-length number
      - unknown-message-type number
      - unknown-tlv number
      - unsupported-address-family number
      - sessions-terminated-holdtime-expiry number
      - total-discovery-interfaces number
      - total-hello-adjacencies number
      - total-peers number
+ linux
+ export-neighbors boolean
+ export-routes boolean
+ import-routes boolean
+ ospf
+ instance name string
+ address-family identityref
+ admin-state keyword
+ advertise-router-capability keyword
+ area area-id
  - active-interfaces number
+ advertise-router-capability boolean
  - area-bdr-rtr-count
+ area-range ip-prefix-mask (ipv4-prefix | ipv6-prefix)
  + advertise boolean
  - as-bdr-rtr-count
+ blackhole-aggregate boolean
+ export-policy reference
  - full-spf-runs
+ interface interface-name reference
  + admin-state keyword
  + advertise-router-capability boolean
  + advertise-subnet boolean
  + authentication
    + keychain reference
  - bad-packets
    - auth-failures

```

```

- bad-area
- bad-auth-type
- bad-checksum
- bad-dead-interval
- bad-dest-address
- bad-hello-interval
- bad-length
- bad-neighbors
- bad-network
- bad-options
- bad-packet-type
- bad-version
- bad-virtual-link
- bdr-id
+ dead-interval number
- dr-id
- events
+ failure-detection
+ enable-bfd boolean
+ hello-interval number
+ interface-type keyword
- last-enabled-time
- last-event-time string
+ ldp-synchronization
+ disable
- duration number
+ end-of-lib boolean
+ hold-down-timer number
- sync-state keyword
- link-lsa-cksum-sum string
- link-lsa-count
+ local-ip-address (ipv4-address | ipv6-address)
+ lsa-filter-out keyword
- lsa-totals
- e-link-lsa
- link-lsa
- link-opaque-lsa
- router-info-lsa
+ metric number
+ mtu number
- neighbor router-id
- address (ipv4-address | ipv6-address-with-zone)
- adjacency-state identityref
- backup-designated-router
- dead-time number
- designated-router
- last-established-time number
- last-event-time
- last-restart-time
- optional-capabilities
- priority number
- restart-helper-age number
- restart-helper-exit-rc keyword
- restart-helper-status keyword
- restart-reason (number | keyword)
- retransmission-queue-length number
- state-changes number
- statistics
- bad-mtu
- bad-nbr-states
- bad-packets
- bad-seq-nums
- duplicates
- events
- lsa-install-failed
- lsa-not-in-lsdbs

```

```

- num-restarts
- option-mismatches
- up-time number
- neighbor-count
- oper-state keyword
- packets
  - discarded
  - retransmits
  - rx-db-description
  - rx-hello
  - rx-ls-ack
  - rx-ls-request
  - rx-ls-update
  - rx-total
  - tx-db-description
  - tx-hello
  - tx-ls-ack
  - tx-ls-request
  - tx-ls-update
  - tx-total
+ passive boolean
+ priority number
+ retransmit-interval number
+ trace-options
  + trace
    + adjacencies
    + interfaces
    + packet
      + detail
      + modifier keyword
      + type keyword
+ transit-delay number
- type keyword
- last-spf-run-time
- lsa-filter-totals
  - export-filtered
  - import-filtered
- lsa-totals
  - area-opaque-lsa
  - asbr-summary-lsa
  - e-inter-area-prefix-lsa
  - e-inter-area-router-lsa
  - e-intra-area-prefix-lsa
  - e-network-lsa
  - e-nssa-lsa
  - e-router-lsa
  - inter-area-prefix-lsa
  - inter-area-router-lsa
  - intra-area-prefix-lsa
  - network-lsa
  - network-summary-lsa
  - nssa-lsa
  - router-info-lsa
  - router-lsa
  - total
  - total-lsa-cksum-sum string
  - unknown-lsa
+ nssa
  + area-range ip-prefix-mask (ipv4-prefix | ipv6-prefix)
  + 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
- extern-lsa-cksum-sum string
- extern-lsa-count
+ external-db-overflow
+ interval number
+ limit number
+ external-preference number
+ graceful-restart
+ helper-mode boolean
+ strict-lsa-checking boolean
+ instance-id number
- 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
+ ldp-synchronization
+ end-of-lib boolean
+ hold-down-timer number
- lsa-totals
- as-external-lsa
- as-opaque-lsa
- e-as-external-lsa
- router-info-lsa
+ max-ecmp-paths number
- new-lsas-originated
- new-lsas-received
- opaque-lsa-support boolean
- oper-state keyword
- overflow boolean
+ overload
+ active boolean
+ overload-include-ext-1 boolean
+ overload-include-ext-2 boolean
+ overload-include-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
- routes-submitted
- spf
- avg-spf-run-interval number
- ext-spf-runs
- full-spf-runs

```

```

- incremental-ext-spf-runs
- incremental-inter-spf-runs
- 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
+ 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
+ trace-options
+ trace
  + adjacencies
  + graceful-restart
  + interfaces
  + lsdbs
  + link-state-id string
  + router-id string
  + type keyword
+ misc
+ packet
  + detail
  + modifier keyword
  + type keyword
+ routes
  + dest-address (ipv4-address | ipv6-address)
+ spf
  + dest-address (ipv4-address | ipv6-address)
+ version identityref
- route-table
- ipv4-unicast
  - route ipv4-prefix string route-type identityref route-owner string id number
  - active boolean
  - fib-programming
    - last-failed-complexes string
    - last-failed-operation-type keyword
    - last-successful-operation-timestamp string
    - last-successful-operation-type keyword
    - pending-operation-type keyword
  - gribi-metadata binary
  - last-app-update string
  - metric number
  - next-hop-group reference
  - next-hop-group-network-instance reference
  - preference number
  - resilient-hash boolean
  - route-summary

```

```

- route-type ip-route-type-name identityref
  - active-routes number
- statistics
  - active-routes number
  - active-routes-with-ecmp number
  - fib-failed-routes number
  - resilient-hash-routes number
  - total-routes number
- ipv6-unicast
- route ipv6-prefix string route-type identityref route-owner string id number
  - active boolean
  - fib-programming
    - last-failed-complexes string
    - last-failed-operation-type keyword
    - last-successful-operation-timestamp string
    - last-successful-operation-type keyword
    - pending-operation-type keyword
  - gribi-metadata binary
  - last-app-update string
  - metric number
  - next-hop-group reference
  - next-hop-group-network-instance reference
  - preference number
  - resilient-hash boolean
- route-summary
  - route-type ip-route-type-name identityref
  - active-routes number
- statistics
  - active-routes number
  - active-routes-with-ecmp number
  - fib-failed-routes number
  - resilient-hash-routes number
  - total-routes number
- mpls
- label-entry label-value number
  - entry-type identityref
  - last-app-update string
  - next-hop-group reference
  - next-network-instance reference
  - operation keyword
- statistics
  - active-entries number
- next-hop index number
- ip-address (ipv4-address | ipv6-address)
- mpls
  - pushed-mpls-label-stack (number | keyword)
- network-instance reference
- programmed-index number
- resolving-route
  - ip-prefix (ipv4-prefix | ipv6-prefix)
  - route-owner string
  - route-type identityref
- resolving-tunnel
  - ip-prefix (ipv4-prefix | ipv6-prefix)
  - tunnel-owner string
  - tunnel-type identityref
- subinterface reference
- type identityref
- vxlan
  - destination-mac string
  - source-mac string
  - vni number
- next-hop-group index number
  - backup-next-hop-group reference
  - fib-programming
    - last-failed-complexes string

```

```

- last-failed-operation-type keyword
- last-successful-operation-timestamp string
- last-successful-operation-type keyword
- pending-operation-type keyword
- next-hop id number
- next-hop reference
- resolved keyword
- weight number
- programmed-index number
+ router-id string
+ segment-routing
+ mpls
- sid-database
- prefix-sid prefix (ipv4-prefix | ipv6-prefix) sid-label-
value number protocol keyword protocol-instance number protocol-multi-
topology number algorithm number
- active boolean
- prefix-conflict boolean
- sid-conflict boolean
+ static-routes
+ route prefix (ipv4-prefix | ipv6-prefix)
+ admin-state keyword
- installed boolean
+ metric number
+ next-hop-group reference
+ preference number
- system-ipv4-address
- oper-down-reason keyword
- oper-state keyword
- system-ipv6-address
- oper-down-reason keyword
- oper-state keyword
- 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
- tunnel-table
- ipv4
- statistics
- active-tunnels number
- inactive-tunnels number
- total-tunnels number
- tunnel ipv4-prefix string type identityref owner string id number
- encapsulation-type keyword
- fib-programming
- not-programmed-reason keyword
- status keyword
- last-app-update string
- metric number
- next-hop-group reference
- preference number
- vxlan

```

```

- destination-address (ipv4-address | ipv6-address)
- destination-udp-port number
- source-address (ipv4-address | ipv6-address)
- time-to-live number
- tunnel-summary
  - tunnel-type type identityref
  - active-tunnels number
  - inactive-tunnels number
  - total-tunnels number
- ipv6
  - statistics
    - active-tunnels number
    - inactive-tunnels number
    - total-tunnels number
  - tunnel ipv6-prefix string type identityref owner string id number
  - encapsulation-type keyword
  - fib-programming
    - not-programmed-reason keyword
    - status keyword
  - last-app-update string
  - metric number
  - next-hop-group reference
  - preference number
  - vxlan
    - destination-address (ipv4-address | ipv6-address)
    - destination-udp-port number
    - source-address (ipv4-address | ipv6-address)
    - time-to-live number
  - tunnel-summary
    - tunnel-type type identityref
    - active-tunnels number
    - inactive-tunnels number
    - total-tunnels 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
+ vxlan-interface name string
  - oper-down-reason keyword
  - oper-state keyword

```

6.1 network-instance Descriptions

network-instance *name string*

Description	Network instances configured on the local system
Context	network-instance name string
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	A unique name identifying the network instance
Context	network-instance name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	This leaf contains the configured, desired state of the network instance.
Context	network-instance name string admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

aggregate-routes

Description	Enable the aggregate-routes context
Context	network-instance name string aggregate-routes
Tree	aggregate-routes
Configurable	True

Platforms Supported on all platforms

route prefix (*ipv4-prefix* | *ipv6-prefix*)

Description Enter the route list instance

Context [network-instance name](#) *string* [aggregate-routes](#) [route prefix](#) (*ipv4-prefix* | *ipv6-prefix*)

Tree [route](#)

Configurable True

Platforms Supported on all platforms

Max. Elements 16384

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description Enter the prefix context

Context [network-instance name](#) *string* [aggregate-routes](#) [route prefix](#) (*ipv4-prefix* | *ipv6-prefix*)

Configurable True

Platforms Supported on all platforms

admin-state *keyword*

Description This leaf contains the configured, desired state of the aggregate prefix.

Context [network-instance name](#) *string* [aggregate-routes](#) [route prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [admin-state](#) *keyword*

Tree [admin-state](#)

Default enable

Options

- enable
- disable

Configurable True

Platforms Supported on all platforms

aggregator

Description Enter the aggregator context

Context [network-instance name](#) *string* [aggregate-routes](#) [route prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [aggregator](#)

Tree [aggregator](#)

Configurable	True
Platforms	Supported on all platforms

address string

Description	Specifies the aggregator's IP address.
Context	network-instance name string aggregate-routes route prefix (ipv4-prefix ipv6-prefix) aggregator address string
Tree	address
Configurable	True
Platforms	Supported on all platforms

as-number number

Description	Specifies the aggregator's ASN
Context	network-instance name string aggregate-routes route prefix (ipv4-prefix ipv6-prefix) aggregator as-number number
Tree	as-number
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

communities

Description	Enter the communities context
Context	network-instance name string aggregate-routes route prefix (ipv4-prefix ipv6-prefix) communities
Tree	communities
Configurable	True
Platforms	Supported on all platforms

add (bgp-std-community-type | bgp-std-community-regexp-type | identityref | bgp-large-community-type | bgp-large-community-regexp-type)

Description	Enter the add context
Context	network-instance name string aggregate-routes route prefix (ipv4-prefix ipv6-prefix) communities add (bgp-std-community-type bgp-std-community-regexp-type identityref bgp-large-community-type bgp-large-community-regexp-type)

Tree	add
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
Platforms	Supported on all platforms
Max. Elements	12

generate-icmp *boolean*

Description	When set to true, the router generates ICMP unreachable messages for packets matching the aggregate route (and not a more specific route).
Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) generate-icmp <i>boolean</i>
Tree	generate-icmp
Configurable	True
Platforms	Supported on all platforms

installed *boolean*

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
Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) installed <i>boolean</i>
Tree	installed
Configurable	False
Platforms	Supported on all platforms

summary-only *boolean*

Description	When set to true the router blocks the advertisement of all contributing routes of this aggregate route in dynamic protocols such as BGP.
Context	network-instance name <i>string</i> aggregate-routes route prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) summary-only <i>boolean</i>
Tree	summary-only
Default	false
Configurable	True
Platforms	Supported on all platforms

bgp-rib

Description	Container for BGP RIB state.
Context	network-instance name <i>string</i> bgp-rib
Tree	bgp-rib
Configurable	False
Platforms	Supported on all platforms

attr-sets

Description	Container for BGP RIB path attribute sets that can be shared by one or more BGP routes.
Context	network-instance name <i>string</i> bgp-rib attr-sets
Tree	attr-sets
Configurable	False
Platforms	Supported on all platforms

attr-set [attr-set-type](#) *keyword* [index](#) *number*

Description	List of attribute sets.
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
Configurable	False
Platforms	Supported on all platforms

attr-set-type *keyword*

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.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index number
Options	<ul style="list-style-type: none"> • rib-in • rib-out
Configurable	False
Platforms	Supported on all platforms

index number

Description	A unique internal identifier of the attribute set.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index number
Configurable	False
Platforms	Supported on all platforms

aggregator

Description	Enter the aggregator context
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index number aggregator
Tree	aggregator
Configurable	False
Platforms	Supported on all platforms

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

Description	The router ID of the BGP router that formed the aggregate route.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index number aggregator address (ipv4-address ipv6-address)
Tree	address
Configurable	False
Platforms	Supported on all platforms

as-number *number*

Description	The 2byte or 4byte AS number of the router that formed the aggregate route.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> aggregator as-number <i>number</i>
Tree	as-number
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

aigp *number*

Description	The value in the AIGP path attribute.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> aigp <i>number</i>
Tree	aigp
Configurable	False
Platforms	Supported on all platforms

as-path

Description	A container for the AS path attribute of the attribute set.
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
Tree	as-path
Configurable	False
Platforms	Supported on all platforms

segment [as-path-index](#) *number*

Description	A list of segments. Each segment has a type and a list of one or more AS numbers.
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>
Tree	segment
Configurable	False
Platforms	Supported on all platforms

as-path-index *number*

Description	RIB attribute AS Path index
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>
Configurable	False
Platforms	Supported on all platforms

member *number*

Description	A list of AS numbers (each of which is a 2byte-ASN or a 4byte-ASN) that belong to the AS path segment.
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> member <i>number</i>
Tree	member
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

type *keyword*

Description	The type of the AS path segment.
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
Options	<ul style="list-style-type: none"> • as-set • as-sequence • as-confed-sequence • as-confed-set
Configurable	False
Platforms	Supported on all platforms

atomic-aggregate *boolean*

Description	Set to true to indicate the presence of the ATOMIC_AGGREGATE path attribute.
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

Configurable	False
Platforms	Supported on all platforms

cluster-list (*ipv4-address* | *ipv6-address*)

Description	The list of IPv4 addresses in the CLUSTER_LIST path attribute.
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number cluster-list (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	cluster-list
Configurable	False
Platforms	Supported on all platforms

communities

Description	Container for different types of BGP communities
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number communities
Tree	communities
Configurable	False
Platforms	Supported on all platforms

community *string*

Description	List of standard 4-byte community values in the COMMUNITY path attribute. Each should be displayed in the format <0..65355>:<0..65535>
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number communities community <i>string</i>
Tree	community
Configurable	False
Platforms	Supported on all platforms

ext-community *string*

Description	List of extended 8-byte community values in the COMMUNITY path attribute.
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number communities ext-community <i>string</i>
Tree	ext-community
Configurable	False

Platforms Supported on all platforms

large-community *string*

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>

Context [network-instance name](#) [string](#) [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) [keyword](#) [index](#) [number](#) [communities](#) [large-community](#) [string](#)

Tree [large-community](#)

String Length 1 to 72

Configurable False

Platforms Supported on all platforms

local-pref *number*

Description The value of the LOCAL_PREF path attribute.

Context [network-instance name](#) [string](#) [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) [keyword](#) [index](#) [number](#) [local-pref](#) [number](#)

Tree [local-pref](#)

Configurable False

Platforms Supported on all platforms

med *number*

Description The value of the MULTI_EXIT_DISC path attribute.

Context [network-instance name](#) [string](#) [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) [keyword](#) [index](#) [number](#) [med](#) [number](#)

Tree [med](#)

Configurable False

Platforms Supported on all platforms

next-hop (*ipv4-address* | *ipv6-address-with-zone*)

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).

Context [network-instance name](#) [string](#) [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) [keyword](#) [index](#) [number](#) [next-hop](#) ([ipv4-address](#) | [ipv6-address-with-zone](#))

Tree [next-hop](#)

Configurable	False
Platforms	Supported on all platforms

origin keyword

Description	The value of the ORIGIN path attribute
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number origin keyword
Tree	origin
Options	<ul style="list-style-type: none"> • igp • egp • incomplete
Configurable	False
Platforms	Supported on all platforms

originator-id (ipv4-address | ipv6-address)

Description	The address in the ORIGINATOR_ID attribute added by a route reflector.
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number originator-id (ipv4-address ipv6-address)
Tree	originator-id
Configurable	False
Platforms	Supported on all platforms

pmsi-tunnel

Description	A container for the Provider Multicast Service Interface Tunnel Attribute (PTA) of the attribute set.
Context	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number pmsi-tunnel
Tree	pmsi-tunnel
Configurable	False
Platforms	Supported on all platforms

flags

Description	A container for the PTA Flags
--------------------	-------------------------------

Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel flags
Tree	flags
Configurable	False
Platforms	Supported on all platforms

assisted-replication-type *keyword*

Description	The value of the assisted-replication role type.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel flags assisted-replication-type <i>keyword</i>
Tree	assisted-replication-type
Options	<ul style="list-style-type: none"> • none • ar-replicator • ar-leaf • reserved
Configurable	False
Platforms	Supported on all platforms

leaf-information-required *boolean*

Description	The value of the Leaf Information Required (LIR) flag.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel flags leaf-information-required <i>boolean</i>
Tree	leaf-information-required
Configurable	False
Platforms	Supported on all platforms

pruned-flood-list

Description	A container for the optimized ingress replication pruned flood list flags.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel flags pruned-flood-list
Tree	pruned-flood-list
Configurable	False
Platforms	Supported on all platforms

broadcast-multicast *keyword*

Description	The value of the broadcast-multicast flag.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel flags pruned-flood-list broadcast-multicast <i>keyword</i>
Tree	broadcast-multicast
Options	<ul style="list-style-type: none"> • 0 • 1
Configurable	False
Platforms	Supported on all platforms

unknown-unicast *keyword*

Description	The value of the unknown-unicast flag.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel flags pruned-flood-list unknown-unicast <i>keyword</i>
Tree	unknown-unicast
Options	<ul style="list-style-type: none"> • 0 • 1
Configurable	False
Platforms	Supported on all platforms

tunnel-endpoint (*ipv4-address* | *ipv6-address*)

Description	The value of the tunnel-endpoint in the PMSI Tunnel Attribute.
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel tunnel-endpoint (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	tunnel-endpoint
Configurable	False
Platforms	Supported on all platforms

tunnel-type *keyword*

Description	The value of the tunnel-type in the PMSI Tunnel Attribute
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel tunnel-type <i>keyword</i>
Tree	tunnel-type

Options	<ul style="list-style-type: none"> • no-tunnel • rsvp-te-p2mp • mldp-p2mp • pim-ssm • pim-sm • bidir-pim • ingress-replication • mldp-mp2mp • assisted-replication • bier
----------------	---

Configurable	False
Platforms	Supported on all platforms

vni number

Description	The VXLAN Network Identifier
Context	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type <i>keyword</i> index <i>number</i> pmsi-tunnel vni <i>number</i>
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

unknown-attributes

Description	Container for unknown path 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
Configurable	False
Platforms	Supported on all platforms

unknown-attribute [unknown-attr-index](#) *number*

Description	List of unknown BGP path 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 unknown-attribute unknown-attr-index <i>number</i>

Tree	unknown-attribute
Configurable	False
Platforms	Supported on all platforms

unknown-attr-index *number*

Description	RIB attribute unknown attribute index
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>
Configurable	False
Platforms	Supported on all platforms

attr-len *number*

Description	The length of the unknown path attribute
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
Configurable	False
Platforms	Supported on all platforms

attr-type *number*

Description	The type code of the unknown path attribute
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
Configurable	False
Platforms	Supported on all platforms

extended *boolean*

Description	Set to true if the unknown path attribute has the extended length flag is set to 1.
--------------------	---

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> extended <i>boolean</i>
Tree	extended
Configurable	False
Platforms	Supported on all platforms

optional *boolean*

Description	Set to true if the unknown path attribute has the optional flag is set to 1.
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> optional <i>boolean</i>
Tree	optional
Configurable	False
Platforms	Supported on all platforms

partial *boolean*

Description	Set to true if the unknown path attribute has the partial flag is set to 1.
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> partial <i>boolean</i>
Tree	partial
Configurable	False
Platforms	Supported on all platforms

transitive *boolean*

Description	Set to true if the unknown path attribute has the transitive flag is set to 1.
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> transitive <i>boolean</i>
Tree	transitive
Configurable	False
Platforms	Supported on all platforms

evpn

Description	Container for RIB state of EVPN routes.
Context	network-instance name <i>string</i> bgp-rib evpn
Tree	evpn
Configurable	False
Platforms	Supported on all platforms

rib-in-out

Description	Container for BGP routes learned and advertised to BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out
Tree	rib-in-out
Configurable	False
Platforms	Supported on all platforms

rib-in-post

Description	Container for the post-import-policy version of BGP routes learned from BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post
Tree	rib-in-post
Configurable	False
Platforms	Supported on all platforms

ethernet-ad-routes [route-distinguisher](#) (*string | string | string | string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address | ipv6-address*)

Description	List of Ethernet AD (Auto-Discovery) routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address ipv6-address</i>)
Tree	ethernet-ad-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string | string | string | string*)

Description	The route distinguisher encoded in the NLRI.
--------------------	--

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier encoded in the NLRI
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index .
--------------------	--

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) best-route <i>boolean</i>
Tree	best-route
Configurable	False
Platforms	Supported on all platforms

group-best *boolean*

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i>

[ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [invalid-reason](#)
[rejected-route](#) *boolean*

Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-as *number*

Description	The last external AS to advertise the route into the local AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor-as <i>number</i>
Tree	neighbor-as
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False

Platforms Supported on all platforms

stale-route *boolean*

Description Set to true if the route is stale due to BGP graceful restart.

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [stale-route](#) *boolean*

Tree [stale-route](#)

Configurable False

Platforms Supported on all platforms

tie-break-reason *keyword*

Description Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [tie-break-reason](#) *keyword*

Tree [tie-break-reason](#)

Options

- unknown
- none
- origin
- as-path-length
- next-hop-cost
- med
- local-pref
- aggregate
- originator-id
- cluster-list
- extended-community
- aigp
- missing-attribute
- rtm-pref
- owner
- eigrp-labeled
- vpn-route
- ebgp-route

- peer-ip
- local-peer
- multi-path
- vpn-rd
- next-hop-type
- invalid-route
- origin-validation
- long-live-gr-stale
- default-originate
- rtm-install-disabled
- peer-router-id
- path-identifier

Configurable

False

Platforms

Supported on all platforms

used-route *boolean***Description**

Indicates true if the route is being used for forwarding.

Context

[network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [used-route](#) *boolean*

Tree[used-route](#)**Configurable**

False

Platforms

Supported on all platforms

valid-route *boolean***Description**

Indicates true if the route is valid.

Context

[network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ethernet-ad-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [valid-route](#) *boolean*

Tree[valid-route](#)**Configurable**

False

Platforms

Supported on all platforms

vni *number***Description**

The VXLAN Network Identifier

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-adj-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address ipv6-address</i>) vni <i>number</i>
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

ethernet-segment-routes [route-distinguisher](#) (*string | string | string | string*) [esi](#) *string* [originating-router](#) (*ipv4-address | ipv6-address*) [neighbor](#) (*ipv4-address | ipv6-address*)

Description	List of Ethernet Segment routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	ethernet-segment-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string | string | string | string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

originating-router (*ipv4-address* | *ipv6-address*)

Description	The IPv4 or IPv6 address of the originating router
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) best-route <i>boolean</i>

Tree	best-route
Configurable	False
Platforms	Supported on all platforms

group-best *boolean*

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i>

	originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-as *number*

Description	The last external AS to advertise the route into the local AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor-as <i>number</i>
Tree	neighbor-as
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False
Platforms	Supported on all platforms

stale-route *boolean*

Description	Set to true if the route is stale due to BGP graceful restart.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) stale-route <i>boolean</i>
Tree	stale-route
Configurable	False
Platforms	Supported on all platforms

tie-break-reason *keyword*

Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Context	network-instance <i>name</i> string bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> • unknown • none • origin • as-path-length • next-hop-cost • med • local-pref • aggregate • originator-id • cluster-list • extended-community • aigp • missing-attribute • rtm-pref • owner • eigrp-labeled • vpn-route • ebgp-route • peer-ip • local-peer • multi-path • vpn-rd • next-hop-type • invalid-route • origin-validation • long-live-gr-stale • default-originate • rtm-install-disabled • peer-router-id

	<ul style="list-style-type: none"> path-identifier
Configurable	False
Platforms	Supported on all platforms

used-route *boolean*

Description	Indicates true if the route is being used for forwarding.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) used-route <i>boolean</i>
Tree	used-route
Configurable	False
Platforms	Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

imet-routes [route-distinguisher](#) (*string* | *string* | *string* | *string*) [originating-router](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*)

Description	List of Inclusive Multicast Ethernet Tag routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	imet-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

originating-router (*ipv4-address* | *ipv6-address*)

Description	The IPv4 or IPv6 address of the originating router
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

best-route boolean

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) best-route <i>boolean</i>
Tree	best-route
Configurable	False
Platforms	Supported on all platforms

group-best boolean

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
--------------------	----------------------------------

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False

Platforms Supported on all platforms

rejected-route *boolean*

Description Indicates true if the route was rejected by an import policy.

Context [network-instance name string](#) [bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher \(string | string | string | string\)](#) [originating-router \(ipv4-address | ipv6-address\)](#) [ethernet-tag-id number](#) [neighbor \(ipv4-address | ipv6-address\)](#) [invalid-reason rejected-route boolean](#)

Tree [rejected-route](#)

Configurable False

Platforms Supported on all platforms

last-modified *string*

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.

Context [network-instance name string](#) [bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher \(string | string | string | string\)](#) [originating-router \(ipv4-address | ipv6-address\)](#) [ethernet-tag-id number](#) [neighbor \(ipv4-address | ipv6-address\)](#) [last-modified string](#)

Tree [last-modified](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

neighbor-as *number*

Description The last external AS to advertise the route into the local AS

Context [network-instance name string](#) [bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher \(string | string | string | string\)](#) [originating-router \(ipv4-address | ipv6-address\)](#) [ethernet-tag-id number](#) [neighbor \(ipv4-address | ipv6-address\)](#) [neighbor-as number](#)

Tree [neighbor-as](#)

Range 1 to 4294967295

Configurable False

Platforms Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False
Platforms	Supported on all platforms

stale-route *boolean*

Description	Set to true if the route is stale due to BGP graceful restart.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) stale-route <i>boolean</i>
Tree	stale-route
Configurable	False
Platforms	Supported on all platforms

tie-break-reason *keyword*

Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> • unknown • none • origin • as-path-length • next-hop-cost • med • local-pref • aggregate • originator-id

- cluster-list
- extended-community
- aigp
- missing-attribute
- rtm-pref
- owner
- eigrp-labeled
- vpn-route
- ebgp-route
- peer-ip
- local-peer
- multi-path
- vpn-rd
- next-hop-type
- invalid-route
- origin-validation
- long-live-gr-stale
- default-originate
- rtm-install-disabled
- peer-router-id
- path-identifier

Configurable

False

Platforms

Supported on all platforms

used-route *boolean***Description**

Indicates true if the route is being used for forwarding.

Context

[network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [originating-router](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [used-route](#) *boolean*

Tree[used-route](#)**Configurable**

False

Platforms

Supported on all platforms

valid-route *boolean***Description**

Indicates true if the route is valid.

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

ip-prefix-routes [route-distinguisher](#) (*string* | *string* | *string* | *string*) [ethernet-tag-id](#) *number* [ip-prefix-length](#) *number* [ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address*)

Description	List of IP prefix routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	ip-prefix-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ip-prefix-length *number*

Description	IP prefix length
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Range	0 to 128
Units	bits
Configurable	False
Platforms	Supported on all platforms

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	The IPv4 or IPv6 prefix
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id <i>reference</i>

Tree	attr-id
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
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) best-route <i>boolean</i>
Tree	best-route
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) esi <i>string</i>
Tree	esi
Configurable	False
Platforms	Supported on all platforms

gateway-ip (*ipv4-address* | *ipv6-address*)

Description	An IP address that encodes an overlay index
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) gateway-ip (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	gateway-ip
Configurable	False
Platforms	Supported on all platforms

group-best *boolean*

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>

Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False

Platforms Supported on all platforms

neighbor-as *number*

Description The last external AS to advertise the route into the local AS

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [ethernet-tag-id number ip-prefix-length number ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address*) [neighbor-as number](#)

Tree [neighbor-as](#)

Range 1 to 4294967295

Configurable False

Platforms Supported on all platforms

pending-delete *boolean*

Description Set to true if the route is marked for deletion.

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [ethernet-tag-id number ip-prefix-length number ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address*) [pending-delete boolean](#)

Tree [pending-delete](#)

Configurable False

Platforms Supported on all platforms

stale-route *boolean*

Description Set to true if the route is stale due to BGP graceful restart.

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [ethernet-tag-id number ip-prefix-length number ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address*) [stale-route boolean](#)

Tree [stale-route](#)

Configurable False

Platforms Supported on all platforms

tie-break-reason *keyword*

Description Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> • unknown • none • origin • as-path-length • next-hop-cost • med • local-pref • aggregate • originator-id • cluster-list • extended-community • aigp • missing-attribute • rtm-pref • owner • eigrp-labeled • vpn-route • ebgp-route • peer-ip • local-peer • multi-path • vpn-rd • next-hop-type • invalid-route • origin-validation • long-live-gr-stale • default-originate • rtm-install-disabled • peer-router-id • path-identifier
Configurable	False
Platforms	Supported on all platforms

used-route *boolean*

Description	Indicates true if the route is being used for forwarding.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) used-route <i>boolean</i>
Tree	used-route
Configurable	False
Platforms	Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

vni *number*

Description	The VXLAN Network Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i>
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

mac-ip-routes [route-distinguisher](#) (*string* | *string* | *string* | *string*) [mac-length](#) *number* [mac-address](#) *string* [ip-address](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*)

Description	List of Mac/IP Advertisement routes
--------------------	-------------------------------------

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	mac-ip-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

mac-length *number*

Description	MAC address length
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Range	0 to 48
Units	bits
Configurable	False
Platforms	Supported on all platforms

mac-address *string*

Description	The MAC address
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP host address
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index <i>number</i>

Configurable	False
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) best-route <i>boolean</i>
Tree	best-route
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) esi <i>string</i>
Tree	esi
Configurable	False
Platforms	Supported on all platforms

group-best *boolean*

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
--------------------	----------------------------------

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason next-hop-unresolved <i>boolean</i>

Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-as *number*

Description	The last external AS to advertise the route into the local AS
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor-as <i>number</i>
Tree	neighbor-as
Range	1 to 4294967295

Configurable	False
Platforms	Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False
Platforms	Supported on all platforms

stale-route *boolean*

Description	Set to true if the route is stale due to BGP graceful restart.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) stale-route <i>boolean</i>
Tree	stale-route
Configurable	False
Platforms	Supported on all platforms

tie-break-reason *keyword*

Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> • unknown • none • origin • as-path-length • next-hop-cost • med

- local-pref
- aggregate
- originator-id
- cluster-list
- extended-community
- aigp
- missing-attribute
- rtm-pref
- owner
- eigrp-labeled
- vpn-route
- ebgp-route
- peer-ip
- local-peer
- multi-path
- vpn-rd
- next-hop-type
- invalid-route
- origin-validation
- long-live-gr-stale
- default-originate
- rtm-install-disabled
- peer-router-id
- path-identifier

Configurable

False

Platforms

Supported on all platforms

used-route *boolean***Description**

Indicates true if the route is being used for forwarding.

Context

[network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [mac-length](#) *number* [mac-address](#) *string* [ip-address](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [used-route](#) *boolean*

Tree[used-route](#)**Configurable**

False

Platforms

Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

vni *number*

Description	The VXLAN Network Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i>
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

rib-in-pre

Description	Container for the pre-import-policy version of BGP routes learned from BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre
Tree	rib-in-pre
Configurable	False
Platforms	Supported on all platforms

ethernet-ad-routes [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*)

Description	List of Ethernet AD (Auto-Discovery) routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)

Tree	ethernet-ad-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier encoded in the NLRI
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False

Platforms Supported on all platforms

attr-id reference

Description Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.

Context [network-instance name](#) *string* [bgp-rib](#) [evpn](#) [rib-in-out](#) [rib-in-pre](#) [ethernet-ad-routes](#) [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [attr-id](#) *reference*

Tree [attr-id](#)

Reference [network-instance name](#) *string* [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) *keyword* [index](#) *number*

Configurable False

Platforms Supported on all platforms

vni number

Description The VXLAN Network Identifier

Context [network-instance name](#) *string* [bgp-rib](#) [evpn](#) [rib-in-out](#) [rib-in-pre](#) [ethernet-ad-routes](#) [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [vni](#) *number*

Tree [vni](#)

Range 0 to 16777215

Configurable False

Platforms Supported on all platforms

ethernet-segment-routes route-distinguisher (*string* | *string* | *string* | *string*) **esi** *string* **originating-router** (*ipv4-address* | *ipv6-address*) **neighbor** (*ipv4-address* | *ipv6-address*)

Description List of Ethernet Segment routes

Context [network-instance name](#) *string* [bgp-rib](#) [evpn](#) [rib-in-out](#) [rib-in-pre](#) [ethernet-segment-routes](#) [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [originating-router](#) (*ipv4-address* | *ipv6-address*) [neighbor](#) (*ipv4-address* | *ipv6-address*)

Tree [ethernet-segment-routes](#)

Configurable False

Platforms Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

originating-router (*ipv4-address* | *ipv6-address*)

Description	The IPv4 or IPv6 address of the originating router
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ethernet-segment-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
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
Platforms	Supported on all platforms

imet-routes [route-distinguisher](#) (*string* | *string* | *string* | *string*) [originating-router](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*)

Description	List of Inclusive Multicast Ethernet Tag routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	imet-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

originating-router (*ipv4-address* | *ipv6-address*)

Description	The IPv4 or IPv6 address of the originating router
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-</i>

	<i>address ipv6-address</i>) <i>ethernet-tag-id number neighbor</i> (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre imet-routes route-distinguisher (<i>string string string string</i>) originating-router (<i>ipv4-address ipv6-address</i>) <i>ethernet-tag-id number neighbor</i> (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre imet-routes route-distinguisher (<i>string string string string</i>) originating-router (<i>ipv4-address ipv6-address</i>) <i>ethernet-tag-id number neighbor</i> (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index .
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre imet-routes route-distinguisher (<i>string string string string</i>) originating-router (<i>ipv4-address ipv6-address</i>) <i>ethernet-tag-id number neighbor</i> (<i>ipv4-address ipv6-address</i>) <i>attr-id reference</i>
Tree	attr-id
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

ip-prefix-routes *route-distinguisher* (*string* | *string* | *string* | *string*) *ethernet-tag-id* *number* *ip-prefix-length* *number* *ip-prefix* (*ipv4-prefix* | *ipv6-prefix*) *neighbor* (*ipv4-address* | *ipv6-address*)

Description	List of IP prefix routes
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	ip-prefix-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ip-prefix-length *number*

Description	IP prefix length
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Range	0 to 128

Units	bits
Configurable	False
Platforms	Supported on all platforms

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	The IPv4 or IPv6 prefix
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index .
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index number
Configurable	False
Platforms	Supported on all platforms

esi string

Description	The Ethernet Segment Identifier
Context	network-instance name string bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) esi string
Tree	esi
Configurable	False
Platforms	Supported on all platforms

gateway-ip (ipv4-address | ipv6-address)

Description	An IP address that encodes an overlay index
Context	network-instance name string bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) gateway-ip (ipv4-address ipv6-address)
Tree	gateway-ip
Configurable	False
Platforms	Supported on all platforms

vni number

Description	The VXLAN Network Identifier
Context	network-instance name string bgp-rib evpn rib-in-out rib-in-pre ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) vni number
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

mac-ip-routes route-distinguisher (string | string | string | string) mac-length number mac-address string ip-address (ipv4-address | ipv6-address) ethernet-tag-id number neighbor (ipv4-address | ipv6-address)

Description	List of Mac/IP Advertisement routes
Context	network-instance name string bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (string string string string) mac-length number mac-

[address](#) *string* [ip-address](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#)
number [neighbor](#) (*ipv4-address* | *ipv6-address*)

Tree	mac-ip-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac- address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

mac-length *number*

Description	MAC address length
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac- address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Range	0 to 48
Units	bits
Configurable	False
Platforms	Supported on all platforms

mac-address *string*

Description	The MAC address
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac- address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP host address
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index <i>number</i>

Configurable	False
Platforms	Supported on all platforms

esi string

Description	The Ethernet Segment Identifier
Context	network-instance name string bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (string string string string) mac-length number mac-address string ip-address (ipv4-address ipv6-address) ethernet-tag-id number neighbor (ipv4-address ipv6-address) esi string
Tree	esi
Configurable	False
Platforms	Supported on all platforms

vni number

Description	The VXLAN Network Identifier
Context	network-instance name string bgp-rib evpn rib-in-out rib-in-pre mac-ip-routes route-distinguisher (string string string string) mac-length number mac-address string ip-address (ipv4-address ipv6-address) ethernet-tag-id number neighbor (ipv4-address ipv6-address) vni number
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

rib-out-post

Description	Container for the post-export-policy version of BGP routes advertised to BGP neighbors.
Context	network-instance name string bgp-rib evpn rib-in-out rib-out-post
Tree	rib-out-post
Configurable	False
Platforms	Supported on all platforms

ethernet-ad-routes [route-distinguisher \(string | string | string | string\)](#) [esi string](#) [ethernet-tag-id number neighbor \(ipv4-address | ipv6-address\)](#)

Description	List of Ethernet AD (Auto-Discovery) routes
--------------------	---

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	ethernet-ad-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier encoded in the NLRI
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
--------------------	--

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index .
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
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
Platforms	Supported on all platforms

next-hop (ipv4-address | ipv6-address)

Description	The advertised BGP next-hop address.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) next-hop (ipv4-address ipv6-address)
Tree	next-hop
Configurable	False
Platforms	Supported on all platforms

vni number

Description	The VXLAN Network Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-ad-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) esi <i>string</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) vni number
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

ethernet-segment-routes route-distinguisher (*string | string | string | string*) **esi** *string*
originating-router (*ipv4-address | ipv6-address*) **neighbor** (*ipv4-address | ipv6-address*)

Description	List of Ethernet Segment routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Tree	ethernet-segment-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string | string | string | string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

esi *string*

Description	The Ethernet Segment Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

originating-router (*ipv4-address | ipv6-address*)

Description	The IPv4 or IPv6 address of the originating router
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ethernet-segment-routes route-distinguisher (<i>string string string string</i>) esi <i>string</i> originating-router (<i>ipv4-address ipv6-address</i>) neighbor (<i>ipv4-address ipv6-address</i>)
Configurable	False

Platforms Supported on all platforms

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

Description If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.

Context [network-instance name](#) *string* [bgp-rib](#) [evpn](#) [rib-in-out](#) [rib-out-post](#) [ethernet-segment-routes](#) [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [originating-router](#) (*ipv4-address* | *ipv6-address*) [neighbor](#) (*ipv4-address* | *ipv6-address*)

Configurable False

Platforms Supported on all platforms

attr-id *reference*

Description Leaf reference to [networkinstance/protocols/bgp/rib/attr-sets/attr-set/index](#).

Context [network-instance name](#) *string* [bgp-rib](#) [evpn](#) [rib-in-out](#) [rib-out-post](#) [ethernet-segment-routes](#) [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [originating-router](#) (*ipv4-address* | *ipv6-address*) [neighbor](#) (*ipv4-address* | *ipv6-address*) [attr-id](#) *reference*

Tree [attr-id](#)

Reference [network-instance name](#) *string* [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) *keyword* [index](#) *number*

Configurable False

Platforms Supported on all platforms

next-hop (*ipv4-address* | *ipv6-address*)

Description The advertised BGP next-hop address.

Context [network-instance name](#) *string* [bgp-rib](#) [evpn](#) [rib-in-out](#) [rib-out-post](#) [ethernet-segment-routes](#) [route-distinguisher](#) (*string* | *string* | *string* | *string*) [esi](#) *string* [originating-router](#) (*ipv4-address* | *ipv6-address*) [neighbor](#) (*ipv4-address* | *ipv6-address*) [next-hop](#) (*ipv4-address* | *ipv6-address*)

Tree [next-hop](#)

Configurable False

Platforms Supported on all platforms

imet-routes **route-distinguisher** (*string* | *string* | *string* | *string*) **originating-router** (*ipv4-address* | *ipv6-address*) **ethernet-tag-id** *number* **neighbor** (*ipv4-address* | *ipv6-address*)

Description	List of Inclusive Multicast Ethernet Tag routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	imet-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

originating-router (*ipv4-address* | *ipv6-address*)

Description	The IPv4 or IPv6 address of the originating router
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) originating-router (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False

Platforms Supported on all platforms

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

Description If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [originating-router](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*)

Configurable False

Platforms Supported on all platforms

attr-id *reference*

Description Leaf reference to [networkinstance/protocols/bgp/rib/attr-sets/attr-set/index](#).

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [originating-router](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [attr-id](#) *reference*

Tree [attr-id](#)

Reference [network-instance name](#) *string* [bgp-rib attr-sets attr-set attr-set-type](#) *keyword* [index](#) *number*

Configurable False

Platforms Supported on all platforms

next-hop (*ipv4-address* | *ipv6-address*)

Description The advertised BGP next-hop address.

Context [network-instance name](#) *string* [bgp-rib evpn rib-in-out rib-out-post imet-routes route-distinguisher](#) (*string* | *string* | *string* | *string*) [originating-router](#) (*ipv4-address* | *ipv6-address*) [ethernet-tag-id](#) *number* [neighbor](#) (*ipv4-address* | *ipv6-address*) [next-hop](#) (*ipv4-address* | *ipv6-address*)

Tree [next-hop](#)

Configurable False

Platforms Supported on all platforms

ip-prefix-routes *route-distinguisher* (*string* | *string* | *string* | *string*) *ethernet-tag-id* *number* *ip-prefix-length* *number* *ip-prefix* (*ipv4-prefix* | *ipv6-prefix*) *neighbor* (*ipv4-address* | *ipv6-address*)

Description	List of IP prefix routes
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	ip-prefix-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ip-prefix-length *number*

Description	IP prefix length
Context	network-instance <i>name</i> <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes <i>route-distinguisher</i> (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id <i>number</i> ip-prefix-length <i>number</i> ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Range	0 to 128

Units	bits
Configurable	False
Platforms	Supported on all platforms

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	The IPv4 or IPv6 prefix
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index .
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) ethernet-tag-id number ip-prefix-length number ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
Reference	network-instance name <i>string</i> bgp-rib attr-sets attr-set attr-set-type keyword index number
Configurable	False
Platforms	Supported on all platforms

esi string

Description	The Ethernet Segment Identifier
Context	network-instance name string bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) esi string
Tree	esi
Configurable	False
Platforms	Supported on all platforms

gateway-ip (ipv4-address | ipv6-address)

Description	An IP address that encodes an overlay index
Context	network-instance name string bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) gateway-ip (ipv4-address ipv6-address)
Tree	gateway-ip
Configurable	False
Platforms	Supported on all platforms

next-hop (ipv4-address | ipv6-address)

Description	The advertised BGP next-hop address.
Context	network-instance name string bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) next-hop (ipv4-address ipv6-address)
Tree	next-hop
Configurable	False
Platforms	Supported on all platforms

vni number

Description	The VXLAN Network Identifier
Context	network-instance name string bgp-rib evpn rib-in-out rib-out-post ip-prefix-routes route-distinguisher (string string string string) ethernet-tag-id number ip-prefix-length number ip-prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address) vni number
Tree	vni

Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

mac-ip-routes route-distinguisher (*string | string | string | string*) **mac-length** *number* **mac-address** *string ip-address (ipv4-address | ipv6-address)* **ethernet-tag-id** *number* **neighbor** (*ipv4-address | ipv6-address*)

Description	List of Mac/IP Advertisement routes
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string string string string</i>) mac-length <i>number</i> mac-address <i>string ip-address (ipv4-address ipv6-address)</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address ipv6-address</i>)
Tree	mac-ip-routes
Configurable	False
Platforms	Supported on all platforms

route-distinguisher (*string | string | string | string*)

Description	The route distinguisher encoded in the NLRI.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string string string string</i>) mac-length <i>number</i> mac-address <i>string ip-address (ipv4-address ipv6-address)</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

mac-length *number*

Description	MAC address length
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string string string string</i>) mac-length <i>number</i> mac-address <i>string ip-address (ipv4-address ipv6-address)</i> ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address ipv6-address</i>)
Range	0 to 48
Units	bits
Configurable	False
Platforms	Supported on all platforms

mac-address *string*

Description	The MAC address
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP host address
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

ethernet-tag-id *number*

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

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

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length number mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id number neighbor (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) attr-id reference
Tree	attr-id
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
Platforms	Supported on all platforms

esi string

Description	The Ethernet Segment Identifier
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) esi string
Tree	esi
Configurable	False
Platforms	Supported on all platforms

next-hop (ipv4-address | ipv6-address)

Description	The advertised BGP next-hop address.
Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) next-hop (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	next-hop
Configurable	False
Platforms	Supported on all platforms

vni number

Description	The VXLAN Network Identifier
--------------------	------------------------------

Context	network-instance name <i>string</i> bgp-rib evpn rib-in-out rib-out-post mac-ip-routes route-distinguisher (<i>string</i> <i>string</i> <i>string</i> <i>string</i>) mac-length <i>number</i> mac-address <i>string</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>) ethernet-tag-id <i>number</i> neighbor (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i>
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

ipv4-unicast

Description	Container for RIB state of IPv4-unicast routes.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast
Tree	ipv4-unicast
Configurable	False
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib
Tree	local-rib
Configurable	False
Platforms	Supported on all platforms

routes [prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address-with-zone*) [origin-protocol](#) [identityref](#)

Description	List of IPv4 routes in the local RIB.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) origin-protocol identityref
Tree	routes
Configurable	False
Platforms	Supported on all platforms

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the prefix context
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) origin-protocol identityref
Configurable	False
Platforms	Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) origin-protocol identityref
Configurable	False
Platforms	Supported on all platforms

origin-protocol *identityref*

Description	If the route was imported from another protocol, this is the protocol name.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) origin-protocol identityref
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd IP route added by ARP ND. • bgp Border Gateway Protocol version 4 • bgp-evpn BGP Ethernet VPN (EVPN) • dhcp IP (default) route added by DHCP. • gribi A gRIBI route • host A host route • isis

- IS-IS
- local
 - A directly connected route
- linux
 - IP route added by the linux kernel.
- ndk1
 - Route added by an agent application using the NDK
- ndk2
 - Route added by an agent application using the NDK
- ospfv2
 - OSPFv2
- ospfv3
 - OSPFv3
- static
 - Locally configured static route

Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/bgp-rib/ attr-sets/attr-set/index
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref best-route <i>boolean</i>
Tree	best-route
Configurable	False

Platforms Supported on all platforms

group-best *boolean*

Description Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [local-rib](#) [routes](#) [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [origin-protocol](#) [identityref](#) [group-best](#) *boolean*

Tree [group-best](#)

Configurable False

Platforms Supported on all platforms

invalid-reason

Description Enter the invalid-reason context

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [local-rib](#) [routes](#) [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [origin-protocol](#) [identityref](#) [invalid-reason](#)

Tree [invalid-reason](#)

Configurable False

Platforms Supported on all platforms

as-loop *boolean*

Description Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [local-rib](#) [routes](#) [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [origin-protocol](#) [identityref](#) [invalid-reason](#) [as-loop](#) *boolean*

Tree [as-loop](#)

Configurable False

Platforms Supported on all platforms

cluster-loop *boolean*

Description Indicates true if the BGP route has a cluster-list loop.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [local-rib](#) [routes](#) [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [origin-protocol](#) [identityref](#) [invalid-reason](#) [cluster-loop](#) *boolean*

Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-as *number*

Description	The last external AS to advertise the route into the local AS
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref neighbor-as <i>number</i>
Tree	neighbor-as
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False
Platforms	Supported on all platforms

stale-route *boolean*

Description	Set to true if the route is stale due to BGP graceful restart.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref stale-route <i>boolean</i>
Tree	stale-route
Configurable	False
Platforms	Supported on all platforms

tie-break-reason *keyword*

Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> unknown

- none
- origin
- as-path-length
- next-hop-cost
- med
- local-pref
- aggregate
- originator-id
- cluster-list
- extended-community
- aigp
- missing-attribute
- rtm-pref
- owner
- eigrp-labeled
- vpn-route
- ebgp-route
- peer-ip
- local-peer
- multi-path
- vpn-rd
- next-hop-type
- invalid-route
- origin-validation
- long-live-gr-stale
- default-originate
- rtm-install-disabled
- peer-router-id
- path-identifier

Configurable

False

Platforms

Supported on all platforms

used-route *boolean*

Description

Indicates true if the route is being used for forwarding.

Context

[network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [local-rib](#) [routes](#) [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [origin-protocol](#) [identityref](#) **used-route** *boolean*

Tree	used-route
Configurable	False
Platforms	Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

rib-in-out

Description	Container for BGP routes learned and advertised to BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out
Tree	rib-in-out
Configurable	False
Platforms	Supported on all platforms

rib-in-post

Description	Container for the post-import-policy version of BGP routes learned from BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post
Tree	rib-in-post
Configurable	False
Platforms	Supported on all platforms

routes [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#))

Description	List of IPv4 routes
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone)
Tree	routes

Configurable	False
Platforms	Supported on all platforms

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the prefix context
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) best-route <i>boolean</i>

Tree	best-route
Configurable	False
Platforms	Supported on all platforms

group-best *boolean*

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
--------------------	--

Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False

Platforms Supported on all platforms

neighbor-as *number*

Description The last external AS to advertise the route into the local AS

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [rib-in-out](#) [rib-in-post](#) [routes prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#) [neighbor-as](#) *number*

Tree [neighbor-as](#)

Range 1 to 4294967295

Configurable False

Platforms Supported on all platforms

pending-delete *boolean*

Description Set to true if the route is marked for deletion.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [rib-in-out](#) [rib-in-post](#) [routes prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#) [pending-delete](#) *boolean*

Tree [pending-delete](#)

Configurable False

Platforms Supported on all platforms

stale-route *boolean*

Description Set to true if the route is stale due to BGP graceful restart.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv4-unicast](#) [rib-in-out](#) [rib-in-post](#) [routes prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#) [stale-route](#) *boolean*

Tree [stale-route](#)

Configurable False

Platforms Supported on all platforms

tie-break-reason *keyword*

Description Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.

Context	<code>network-instance name</code> <i>string</i> <code>bgp-rib</code> <code>ipv4-unicast</code> <code>rib-in-out</code> <code>rib-in-post</code> <code>routes</code> <code>prefix</code> (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) <code>neighbor</code> (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) <code>tie-break-reason</code> <i>keyword</i>
Tree	<code>tie-break-reason</code>
Options	<ul style="list-style-type: none"> • unknown • none • origin • as-path-length • next-hop-cost • med • local-pref • aggregate • originator-id • cluster-list • extended-community • aigp • missing-attribute • rtm-pref • owner • eigrp-labeled • vpn-route • ebgp-route • peer-ip • local-peer • multi-path • vpn-rd • next-hop-type • invalid-route • origin-validation • long-live-gr-stale • default-originate • rtm-install-disabled • peer-router-id • path-identifier
Configurable	False
Platforms	Supported on all platforms

used-route *boolean*

Description	Indicates true if the route is being used for forwarding.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) used-route <i>boolean</i>
Tree	used-route
Configurable	False
Platforms	Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-post routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

rib-in-pre

Description	Container for the pre-import-policy version of BGP routes learned from BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre
Tree	rib-in-pre
Configurable	False
Platforms	Supported on all platforms

routes [prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#)

Description	List of IPv4 routes.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone)
Tree	routes
Configurable	False
Platforms	Supported on all platforms

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the prefix context
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to <code>networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index</code> .
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

rib-out-post

Description	Container for the post-export-policy version of BGP routes advertised to BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post
Tree	rib-out-post
Configurable	False
Platforms	Supported on all platforms

routes prefix (*ipv4-prefix* | *ipv6-prefix*) **neighbor** (*ipv4-address* | *ipv6-address-with-zone*)

Description	List of IPv4 routes.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Tree	routes
Configurable	False
Platforms	Supported on all platforms

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the prefix context
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib ipv4-unicast rib-in-out rib-out-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) attr-id reference
Tree	attr-id
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

Platforms Supported on all platforms

ipv6-unicast

Description Container for RIB state of IPv6-unicast routes.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#)

Tree [ipv6-unicast](#)

Configurable False

Platforms Supported on all platforms

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.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [local-rib](#)

Tree [local-rib](#)

Configurable False

Platforms Supported on all platforms

routes [prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address-with-zone*) [origin-protocol](#) [identityref](#)

Description List of IPv6 routes in the local RIB.

Context [network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [local-rib](#) [routes](#) [prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address-with-zone*) [origin-protocol](#) [identityref](#)

Tree [routes](#)

Configurable False

Platforms Supported on all platforms

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description Enter the prefix context

Context [network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [local-rib](#) [routes](#) [prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address-with-zone*) [origin-protocol](#) [identityref](#)

Configurable False

Platforms Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name string bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref
Configurable	False
Platforms	Supported on all platforms

origin-protocol *identityref*

Description	If the route was imported from another protocol, this is the protocol name.
Context	network-instance name string bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd IP route added by ARP ND. • bgp Border Gateway Protocol version 4 • bgp-evpn BGP Ethernet VPN (EVPN) • dhcp IP (default) route added by DHCP. • gribi A gRIBI route • host A host route • isis IS-IS • local A directly connected route • linux IP route added by the linux kernel. • ndk1 Route added by an agent application using the NDK

- ndk2
Route added by an agent application using the NDK
- ospfv2
OSPFv2
- ospfv3
OSPFv3
- static
Locally configured static route

Configurable

False

Platforms

Supported on all platforms

attr-id *reference***Description**

Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index

Context

[network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [local-rib](#) [routes](#) [prefix](#)
(ipv4-prefix | ipv6-prefix) [neighbor](#) *(ipv4-address | ipv6-address-with-zone)*
[origin-protocol](#) [identityref](#) [attr-id](#) *reference*

Tree[attr-id](#)**Reference**

[network-instance name](#) *string* [bgp-rib](#) [attr-sets](#) [attr-set](#) [attr-set-type](#) *keyword*
[index](#) *number*

Configurable

False

Platforms

Supported on all platforms

best-route *boolean***Description**

Set to true if the route is the BGP best path for the prefix.

Context

[network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [local-rib](#) [routes](#) [prefix](#)
(ipv4-prefix | ipv6-prefix) [neighbor](#) *(ipv4-address | ipv6-address-with-zone)*
[origin-protocol](#) [identityref](#) [best-route](#) *boolean*

Tree[best-route](#)**Configurable**

False

Platforms

Supported on all platforms

group-best *boolean***Description**

Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS

Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop
Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-as *number*

Description	The last external AS to advertise the route into the local AS
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref neighbor-as <i>number</i>

Tree	neighbor-as
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False
Platforms	Supported on all platforms

stale-route *boolean*

Description	Set to true if the route is stale due to BGP graceful restart.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref stale-route <i>boolean</i>
Tree	stale-route
Configurable	False
Platforms	Supported on all platforms

tie-break-reason *keyword*

Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> • unknown • none • origin • as-path-length • next-hop-cost • med

- local-pref
- aggregate
- originator-id
- cluster-list
- extended-community
- aigp
- missing-attribute
- rtm-pref
- owner
- eigrp-labeled
- vpn-route
- ebgp-route
- peer-ip
- local-peer
- multi-path
- vpn-rd
- next-hop-type
- invalid-route
- origin-validation
- long-live-gr-stale
- default-originate
- rtm-install-disabled
- peer-router-id
- path-identifier

Configurable

False

Platforms

Supported on all platforms

used-route *boolean*

Description

Indicates true if the route is being used for forwarding.

Context

[network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [local-rib](#) [routes](#) [prefix](#) ([ipv4-prefix](#) | [ipv6-prefix](#)) [neighbor](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [origin-protocol](#) [identityref](#) [used-route](#) *boolean*

Tree

[used-route](#)

Configurable

False

Platforms

Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast local-rib routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone) origin-protocol identityref valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

rib-in-out

Description	Container for BGP routes learned and advertised to BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out
Tree	rib-in-out
Configurable	False
Platforms	Supported on all platforms

rib-in-post

Description	Container for the post-import-policy version of BGP routes learned from BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post
Tree	rib-in-post
Configurable	False
Platforms	Supported on all platforms

routes [prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#)

Description	List of IPv6 routes
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-with-zone)
Tree	routes
Configurable	False
Platforms	Supported on all platforms

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the prefix context
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

best-route *boolean*

Description	Set to true if the route is the BGP best path for the prefix.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-post routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) best-route <i>boolean</i>
Tree	best-route
Configurable	False
Platforms	Supported on all platforms

group-best *boolean*

Description	Set to true if the route is the best BGP route amongst all routes received from one particular neighbor AS
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-with-zone) group-best <i>boolean</i>
Tree	group-best
Configurable	False
Platforms	Supported on all platforms

invalid-reason

Description	Enter the invalid-reason context
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-with-zone) invalid-reason
Tree	invalid-reason
Configurable	False
Platforms	Supported on all platforms

as-loop *boolean*

Description	Indicates true if the BGP route has an AS path loop that exceeds the configured threshold.
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-with-zone) invalid-reason as-loop <i>boolean</i>
Tree	as-loop
Configurable	False
Platforms	Supported on all platforms

cluster-loop *boolean*

Description	Indicates true if the BGP route has a cluster-list loop.
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-with-zone) invalid-reason cluster-loop <i>boolean</i>
Tree	cluster-loop

Configurable	False
Platforms	Supported on all platforms

next-hop-unresolved *boolean*

Description	Indicates true if the BGP route has a BGP next-hop that cannot be resolved to an outgoing interface.
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-with-zone) invalid-reason next-hop-unresolved <i>boolean</i>
Tree	next-hop-unresolved
Configurable	False
Platforms	Supported on all platforms

rejected-route *boolean*

Description	Indicates true if the route was rejected by an import policy.
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-with-zone) invalid-reason rejected-route <i>boolean</i>
Tree	rejected-route
Configurable	False
Platforms	Supported on all platforms

last-modified *string*

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.
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-with-zone) last-modified <i>string</i>
Tree	last-modified
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-as *number*

Description	The last external AS to advertise the route into the local AS
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-with-zone) neighbor-as <i>number</i>
Tree	neighbor-as
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

pending-delete *boolean*

Description	Set to true if the route is marked for deletion.
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-with-zone) pending-delete <i>boolean</i>
Tree	pending-delete
Configurable	False
Platforms	Supported on all platforms

stale-route *boolean*

Description	Set to true if the route is stale due to BGP graceful restart.
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-with-zone) stale-route <i>boolean</i>
Tree	stale-route
Configurable	False
Platforms	Supported on all platforms

tie-break-reason *keyword*

Description	Indicates the reason why a BGP route is sorted behind the next best route. The BGP best path displays a value of 'none'.
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-with-zone) tie-break-reason <i>keyword</i>
Tree	tie-break-reason
Options	<ul style="list-style-type: none"> unknown

- none
- origin
- as-path-length
- next-hop-cost
- med
- local-pref
- aggregate
- originator-id
- cluster-list
- extended-community
- aigp
- missing-attribute
- rtm-pref
- owner
- eigrp-labeled
- vpn-route
- ebgp-route
- peer-ip
- local-peer
- multi-path
- vpn-rd
- next-hop-type
- invalid-route
- origin-validation
- long-live-gr-stale
- default-originate
- rtm-install-disabled
- peer-router-id
- path-identifier

Configurable

False

Platforms

Supported on all platforms

used-route *boolean*

Description

Indicates true if the route is being used for forwarding.

Context

[network-instance name](#) *string* [bgp-rib](#) [ipv6-unicast](#) [rib-in-out](#) [rib-in-post](#) [routes prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#) **used-route** *boolean*

Tree	used-route
Configurable	False
Platforms	Supported on all platforms

valid-route *boolean*

Description	Indicates true if the route is valid.
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-with-zone) valid-route <i>boolean</i>
Tree	valid-route
Configurable	False
Platforms	Supported on all platforms

rib-in-pre

Description	Container for the pre-import-policy version of BGP routes learned from BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre
Tree	rib-in-pre
Configurable	False
Platforms	Supported on all platforms

routes [prefix \(ipv4-prefix | ipv6-prefix\)](#) [neighbor \(ipv4-address | ipv6-address-with-zone\)](#)

Description	List of IPv6 routes.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone)
Tree	routes
Configurable	False
Platforms	Supported on all platforms

prefix *(ipv4-prefix | ipv6-prefix)*

Description	Enter the prefix context
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (ipv4-prefix ipv6-prefix) neighbor (ipv4-address ipv6-address-with-zone)

Configurable	False
Platforms	Supported on all platforms

neighbor (*ipv4-address* | *ipv6-address-with-zone*)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-in-pre routes prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) neighbor (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) attr-id <i>reference</i>
Tree	attr-id
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
Platforms	Supported on all platforms

rib-out-post

Description	Container for the post-export-policy version of BGP routes advertised to BGP neighbors.
Context	network-instance name <i>string</i> bgp-rib ipv6-unicast rib-in-out rib-out-post
Tree	rib-out-post
Configurable	False
Platforms	Supported on all platforms

routes [prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [neighbor](#) (*ipv4-address* | *ipv6-address-with-zone*)

Description	List of IPv6 routes.
--------------------	----------------------

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-with-zone)
Tree	routes
Configurable	False
Platforms	Supported on all platforms

prefix ([ipv4-prefix](#) | [ipv6-prefix](#))

Description	Enter the prefix context
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-with-zone)
Configurable	False
Platforms	Supported on all platforms

neighbor ([ipv4-address](#) | [ipv6-address-with-zone](#))

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
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-with-zone)
Configurable	False
Platforms	Supported on all platforms

attr-id *reference*

Description	Leaf reference to networkinstance/protocols/bgp/rib/ attr-sets/attr-set/index .
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-with-zone) attr-id reference
Tree	attr-id
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
Platforms	Supported on all platforms

bridge-table

Description	Enable the bridge-table context
Context	network-instance name <i>string</i> bridge-table
Tree	bridge-table
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

discard-unknown-dest-mac *boolean*

Description	Discard frames with unknown destination mac addresses. The source mac address of the discarded frame is learned as long as the mac is valid, mac-learning is enabled, and the number of entries has not reached the maximum-entries threshold.
Context	network-instance name <i>string</i> bridge-table discard-unknown-dest-mac <i>boolean</i>
Tree	discard-unknown-dest-mac
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-duplication

Description	Configuration of the MAC duplication procedures.
Context	network-instance name <i>string</i> bridge-table mac-duplication
Tree	mac-duplication
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action *keyword*

Description	Action to take on the subinterface (if action is use-net-instance-action) upon detecting at least one mac addresses as duplicate on the subinterface. In particular:
Context	network-instance name <i>string</i> bridge-table mac-duplication action <i>keyword</i>
Tree	action
Default	stop-learning
Options	<ul style="list-style-type: none"> • stop-learning • blackhole

	<ul style="list-style-type: none"> oper-down
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

admin-state *keyword*

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.
Context	network-instance name <i>string</i> bridge-table mac-duplication admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> enable disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

duplicate-entries

Description	Enter the duplicate-entries context
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries
Tree	duplicate-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac *address string*

Description	macs duplicate on the bridging instance
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address *string*

Description	Enter the address context
--------------------	---------------------------

Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination *string*

Description	The name of the destination the duplicate MAC it is installed against in the fdb.
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> destination <i>string</i>
Tree	destination
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-index *number*

Description	A system-wide unique identifier of a subinterface object (system allocated).
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
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-type *keyword*

Description	The type of the destination the duplicate MAC is installed against in the fdb.
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
Options	<ul style="list-style-type: none"> • sub-interface • blackhole • irb-interface • vxlan • reserved • evpn-mpls
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dup-detect-time *string*

Description	The date and time when the mac was declared duplicate
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
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

hold-down-time-remaining (*keyword | number*)

Description	Remaining hold down time for duplicate MAC
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> hold-down-time-remaining (<i>keyword number</i>)
Tree	hold-down-time-remaining
Units	seconds
Options	<ul style="list-style-type: none"> indefinite
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

hold-down-time (*keyword | number*)

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.
Context	network-instance name <i>string</i> bridge-table mac-duplication hold-down-time (<i>keyword number</i>)
Tree	hold-down-time
Range	2 to 60
Default	9
Units	minutes
Options	<ul style="list-style-type: none"> indefinite
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

monitoring-window *number*

Description	Monitoring window for detecting duplication on a given mac address. A mac is declared as duplicate if it exceeds the num-moves within the monitoring-window.
Context	network-instance name <i>string</i> bridge-table mac-duplication monitoring-window <i>number</i>
Tree	monitoring-window
Range	1 to 15
Default	3
Units	minutes
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

num-moves *number*

Description	Number of moves a mac is allowed within the monitoring-window, before it is declared duplicate.
Context	network-instance name <i>string</i> bridge-table mac-duplication num-moves <i>number</i>
Tree	num-moves
Range	3 to 10
Default	5
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-learning

Description	Enter the mac-learning context
Context	network-instance name <i>string</i> bridge-table mac-learning
Tree	mac-learning
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

admin-state *keyword*

Description	Configurable state of the learning procedures for dynamic mac addresses. If disabled, the existing macs in the bridge-table will be kept (and refreshed if new frames arrive for them) but no new mac addresses will be learned.
--------------------	--

Frames with unknown mac addresses are not dropped, unless discard-unknown-src-mac is configured.

Context	network-instance name <i>string</i> bridge-table mac-learning admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

aging

Description	Enter the aging context
Context	network-instance name <i>string</i> bridge-table mac-learning aging
Tree	aging
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

admin-state *keyword*

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.
Context	network-instance name <i>string</i> bridge-table mac-learning aging admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

age-time *number*

Description	Configurable aging time for dynamically learned mac addresses
Context	network-instance name <i>string</i> bridge-table mac-learning aging age-time <i>number</i>

Tree	age-time
Range	60 to 86400
Default	300
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

learnt-entries

Description	Enter the learnt-entries context
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries
Tree	learnt-entries
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac *address string*

Description	MACs learnt on the bridging instance
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i>
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address *string*

Description	Enter the address context
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

aging (*number* | *keyword*)

Description	Remaining age time for learnt MACs
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i> aging (<i>number</i> <i>keyword</i>)
Tree	aging

Units	seconds
Options	• disabled
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination *string*

Description	The name of the subinterface where the MAC is learnt against.
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i> destination <i>string</i>
Tree	destination
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-update *string*

Description	The date and time of the last update of this learnt mac
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i> last-update <i>string</i>
Tree	last-update
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-relearn-only *boolean*

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
Context	network-instance name <i>string</i> bridge-table mac-learning mac-relearn-only <i>boolean</i>
Tree	mac-relearn-only
Default	true
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-mac-learning *keyword*

Description	The operational state of mac-learning on this network instance.
--------------------	---

Context	network-instance name <i>string</i> bridge-table mac-learning oper-mac-learning <i>keyword</i>
Tree	oper-mac-learning
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the <code>reinvoke-with-delay</code> action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

oper-mac-learning-disabled-reason *keyword*

Description The reason for the mac-learning being disabled on this network instance

Context [network-instance name](#) *string* [bridge-table mac-learning oper-mac-learning-disabled-reason](#) *keyword*

Tree [oper-mac-learning-disabled-reason](#)

Options

- admin-disabled

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-limit

Description Bridge Table size and thresholds.

Context [network-instance name](#) *string* [bridge-table mac-limit](#)

Tree [mac-limit](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

maximum-entries *number*

Description Maximum number of mac addresses allowed in the bridge-table.

Context [network-instance name](#) *string* [bridge-table mac-limit maximum-entries](#) *number*

Tree [maximum-entries](#)

Range 1 to 8192

Default 250

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

warning-threshold-pct *number*

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%

Context [network-instance name](#) *string* [bridge-table mac-limit warning-threshold-pct](#) *number*

Tree	warning-threshold-pct
Range	6 to 100
Default	95
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-table

Description	Enter the mac-table context
Context	network-instance name <i>string</i> bridge-table mac-table
Tree	mac-table
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac *address string*

Description	MACs learnt on the bridging instance
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i>
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address *string*

Description	Enter the address context
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination *string*

Description	The name of the destination where the MAC is programmed against.
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> destination <i>string</i>
Tree	destination
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-index *number*

Description	A system-wide unique identifier of a subinterface object (system allocated).
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> destination-index <i>number</i>
Tree	destination-index
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination-type *keyword*

Description	The type of the destination the MAC installed against in the fdb.
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> destination-type <i>keyword</i>
Tree	destination-type
Options	<ul style="list-style-type: none"> • sub-interface • blackhole • irb-interface • vxlan • reserved • evpn-mpls
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

failed-slots *number*

Description	The list of slot IDs corresponding to the linecards that did not successfully program the mac
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> failed-slots <i>number</i>
Tree	failed-slots
Range	1 to 8
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

is-protected *boolean*

Description	Indicates if the mac is protected in the hardware.
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> is-protected <i>boolean</i>
Tree	is-protected
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-update *string*

Description	The date and time of the last update of this mac
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> last-update <i>string</i>
Tree	last-update
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

not-programmed-reason *keyword*

Description	The reason why the mac is not programmed
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
Options	<ul style="list-style-type: none"> • mac-limit • failed-on-slots • no-destination-index • reserved
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

type *keyword*

Description	The type of the MAC installed in the fib.
Context	network-instance name <i>string</i> bridge-table mac-table mac address <i>string</i> type <i>keyword</i>
Tree	type

Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

protect-anycast-gw-mac *boolean*

Description	Protect anycast gateway mac's installed in the FDB, when this mac-vrf is part of an IRB.
Context	network-instance name <i>string</i> bridge-table protect-anycast-gw-mac <i>boolean</i>
Tree	protect-anycast-gw-mac
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

reserved-macs

Description	Enter the reserved-macs context
Context	network-instance name <i>string</i> bridge-table reserved-macs
Tree	reserved-macs
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac [address](#) *string*

Description	Reserved MACs on the bridging instance
Context	network-instance name <i>string</i> bridge-table reserved-macs mac address <i>string</i>

Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Enter the address context
Context	network-instance name string bridge-table reserved-macs mac address string
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

users application string

Description	Applications reserving this MAC
Context	network-instance name string bridge-table reserved-macs mac address string users application string
Tree	users
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

application string

Description	Enter the application context
Context	network-instance name string bridge-table reserved-macs mac address string users application string
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

static-mac

Description	Enter the static-mac context
Context	network-instance name string bridge-table static-mac
Tree	static-mac
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac address string

Description	Static MACs configured on the bridging instance
Context	network-instance name string bridge-table static-mac mac address string
Tree	mac
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

address string

Description	Enter the address context
Context	network-instance name string bridge-table static-mac mac address string
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

destination (keyword | reference)

Description	The destination where the MAC is programmed against.
Context	network-instance name string bridge-table static-mac mac address string destination (keyword reference)
Tree	destination
Options	<ul style="list-style-type: none"> • blackhole
Reference	network-instance name string interface name string
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	network-instance name string bridge-table statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

active-entries number

Description	The total number of entries that are active in the mac-table.
--------------------	---

Context	network-instance name <i>string</i> bridge-table statistics active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

failed-entries *number*

Description	The total number of macs, which have not been programmed on atleast one slot
Context	network-instance name <i>string</i> bridge-table statistics failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

mac-type *type keyword*

Description	The type of the MAC installed in the fib.
Context	network-instance name <i>string</i> bridge-table statistics mac-type <i>type keyword</i>
Tree	mac-type
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

type *keyword*

Description	Enter the type context
Context	network-instance name <i>string</i> bridge-table statistics mac-type <i>type keyword</i>
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved

	<ul style="list-style-type: none"> • eth-cfm • roe
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

active-entries *number*

Description	The total number of entries of this type that are active in the mac-table.
Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i> active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

failed-entries *number*

Description	The total number of macs of this type, which have not been programmed on atleast one slot
Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i> failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-entries *number*

Description	The total number of macs of this type , active and inactive, that are present in the mac-table.
Context	network-instance name <i>string</i> bridge-table statistics mac-type type <i>keyword</i> total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-entries *number*

Description	The total number of macs, active and inactive, that are present in the mac-table.
Context	network-instance name <i>string</i> bridge-table statistics total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

description *string*

Description	A user-entered description of this network instance.
Context	network-instance name <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

icmp

Description	Enter the icmp context
Context	network-instance name <i>string</i> icmp
Tree	icmp
Configurable	False
Platforms	Supported on all platforms

statistics

Description	ICMP version 4 statistics
Context	network-instance name <i>string</i> icmp statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Timestamp of the last time the interface counters were cleared.
Context	network-instance name <i>string</i> icmp statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

total

Description	Aggregate statistics, counting all ICMP message types
Context	network-instance name <i>string</i> icmp statistics total
Tree	total
Configurable	False
Platforms	Supported on all platforms

in-error-packets *number*

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.)
Context	network-instance name <i>string</i> icmp statistics total in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-packets *number*

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.
Context	network-instance name <i>string</i> icmp statistics total in-packets <i>number</i>
Tree	in-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-error-packets *number*

Description	The number of ICMPv4 messages that could not be sent from this network instance due to issues such as 'no route to the source' or 'fragmentation required but not supported'
Context	network-instance name string icmp statistics total out-error-packets number
Tree	out-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-packets *number*

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.
Context	network-instance name string icmp statistics total out-packets number
Tree	out-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

type [name](#) *keyword*

Description	Enter the type list instance
Context	network-instance name string icmp statistics type name keyword
Tree	type
Configurable	False
Platforms	Supported on all platforms

name *keyword*

Description	Enter the name context
Context	network-instance name string icmp statistics type name keyword
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
Platforms	Supported on all platforms

in-packets *number*

Description	The total number of ICMPv4 messages of this type that the network instance received and extracted successfully to the CPM.
Context	network-instance name <i>string</i> icmp statistics type name <i>keyword</i> in-packets number
Tree	in-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-error-packets *number*

Description	The number of ICMPv4 messages of this type that could not be sent from this network instance due to issues such as 'no route to the source' or 'fragmentation required but not supported'
Context	network-instance name <i>string</i> icmp statistics type name <i>keyword</i> out-error-packets number
Tree	out-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-packets *number*

Description	The total number of ICMPv4 messages of this type that the network instance attempted to send.
Context	network-instance name <i>string</i> icmp statistics type name <i>keyword</i> out-packets number
Tree	out-packets

Default	0
Configurable	False
Platforms	Supported on all platforms

icmp6

Description	Enter the icmp6 context
Context	network-instance name <i>string</i> icmp6
Tree	icmp6
Configurable	False
Platforms	Supported on all platforms

statistics

Description	ICMP version 6 statistics
Context	network-instance name <i>string</i> icmp6 statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Timestamp of the last time the interface counters were cleared.
Context	network-instance name <i>string</i> icmp6 statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

total

Description	Aggregate statistics, counting all ICMP message types
Context	network-instance name <i>string</i> icmp6 statistics total
Tree	total
Configurable	False
Platforms	Supported on all platforms

in-error-packets *number*

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.)
Context	network-instance name <i>string</i> icmp6 statistics total in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-packets *number*

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.
Context	network-instance name <i>string</i> icmp6 statistics total in-packets <i>number</i>
Tree	in-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-error-packets *number*

Description	The number of ICMPv6 messages that could not be sent from this network instance due to issues such as 'no route to the source'
Context	network-instance name <i>string</i> icmp6 statistics total out-error-packets <i>number</i>
Tree	out-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-packets *number*

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.
Context	network-instance name <i>string</i> icmp6 statistics total out-packets <i>number</i>

Tree	out-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

type name keyword

Description	Enter the type list instance
Context	network-instance name string icmp6 statistics type name keyword
Tree	type
Configurable	False
Platforms	Supported on all platforms

name keyword

Description	Enter the name context
Context	network-instance name string icmp6 statistics type name keyword
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 • redirect
Configurable	False
Platforms	Supported on all platforms

in-packets number

Description	The total number of ICMPv6 messages of this type that the network instance received and extracted successfully to the CPM.
Context	network-instance name string icmp6 statistics type name keyword in-packets number

Tree	in-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-error-packets *number*

Description	The number of ICMPv6 messages of this type that could not be sent from this network instance due to issues such as 'no route to the source'
Context	network-instance name <i>string</i> icmp6 statistics type name <i>keyword</i> out-error-packets <i>number</i>
Tree	out-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-packets *number*

Description	The total number of ICMPv6 messages of this type that the network instance attempted to send.
Context	network-instance name <i>string</i> icmp6 statistics type name <i>keyword</i> out-packets <i>number</i>
Tree	out-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

interface *name string*

Description	List of subinterfaces used by this network-instance
Context	network-instance name <i>string</i> interface name <i>string</i>
Tree	interface
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Identifier of sub-interface used in this network-instance
--------------------	---

Context	network-instance name string interface name string
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

index number

Description	The network instance allocated sub interface index
Context	network-instance name string interface name string index number
Tree	index
Default	0
Configurable	False
Platforms	Supported on all platforms

mac-relearn-only boolean

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
Context	network-instance name string interface name string mac-relearn-only boolean
Tree	mac-relearn-only
Default	true
Configurable	False
Platforms	Supported on all platforms

multicast-forwarding keyword

Description	The type of multicast data forwarded by this subinterface.
Context	network-instance name string interface name string multicast-forwarding keyword
Tree	multicast-forwarding
Options	<ul style="list-style-type: none"> • none • BUM • unknown-unicast • broadcast-mcast
Configurable	False
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The reason for the interface being down in the network-instance
Context	network-instance name <i>string</i> interface name <i>string</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
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 • ip-vrf-association-missing • associated-ip-vrf-down • evpn-mh-standby
Configurable	False
Platforms	Supported on all platforms

oper-mac-learning *keyword*

Description	The operational state of mac-learning on this subinterface.
Context	network-instance name <i>string</i> interface name <i>string</i> oper-mac-learning <i>keyword</i>
Tree	oper-mac-learning
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

oper-mac-learning-disabled-reason *keyword*

Description	The reason for the mac-learning being disabled on this interface
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
Options	<ul style="list-style-type: none"> • routed • admin-disabled • mac-dup-detected
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of this subinterface.
Context	network-instance name <i>string</i> interface name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the <code>reinvoke-with-delay</code> action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

ip-forwarding

Description	Forwarding options that apply to the entire network instance.
Context	network-instance name <i>string</i> ip-forwarding
Tree	ip-forwarding
Configurable	True
Platforms	Supported on all platforms

last-resort-lookup

Description	Enter the last-resort-lookup context
Context	network-instance name <i>string</i> ip-forwarding last-resort-lookup
Tree	last-resort-lookup
Configurable	True
Platforms	Supported on all platforms

network-instance *reference*

Description	A reference to another network-instance in which the system will try to find a matching IP route if this network instance does not have any route to the destination IP
Context	network-instance name <i>string</i> ip-forwarding last-resort-lookup network-instance <i>reference</i>
Tree	network-instance
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

receive-ipv4-check *boolean*

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.
--------------------	---

Context	network-instance name <i>string</i> ip-forwarding receive-ipv4-check <i>boolean</i>
Tree	receive-ipv4-check
Configurable	True
Platforms	Supported on all platforms

receive-ipv6-check *boolean*

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.
Context	network-instance name <i>string</i> ip-forwarding receive-ipv6-check <i>boolean</i>
Tree	receive-ipv6-check
Configurable	True
Platforms	Supported on all platforms

ip-load-balancing

Description	Container for IP load-balancing options that are specific to the network-instance
Context	network-instance name <i>string</i> ip-load-balancing
Tree	ip-load-balancing
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

resilient-hash-prefix [ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*)

Description	List of IPv4 and IPv6 prefixes which should be programmed for resilient ECMP hashing.
Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Tree	resilient-hash-prefix
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

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.
Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

hash-buckets-per-path *number*

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.
Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) hash-buckets-per-path <i>number</i>
Tree	hash-buckets-per-path
Range	1 to 32
Default	1
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

max-paths *number*

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.
Context	network-instance name <i>string</i> ip-load-balancing resilient-hash-prefix ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) max-paths <i>number</i>
Tree	max-paths
Range	1 to 64
Default	1
Configurable	True

Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
------------------	--

mpls

Description	Enable the mpls context
Context	network-instance name <i>string</i> mpls
Tree	mpls
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

icmp-tunneling *boolean*

Description	<p>When enabled, ICMP messages generated by the router acting in the role of a transit LSR are injected in the forward direction of the LSP, to be turned around and sent back to the sender of the IP payload by the egress LER.</p> <p>If a transit LSR receives an MPLS packet that cannot be forwarded (e.g. label TTL has expired, or the egress subinterface MPLS MTU was exceeded) and the MPLS packet has an IP payload, the router will generate an appropriate ICMP error message. When icmp-tunneling is 'false' the ICMP error message is dropped if there is no IP route back to the source in the network-instance that received the MPLS packet.</p>
Context	network-instance name <i>string</i> mpls icmp-tunneling <i>boolean</i>
Tree	icmp-tunneling
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

static-entry [top-label](#) *number* [preference](#) *number*

Description	Enter the static-entry list instance
Context	network-instance name <i>string</i> mpls static-entry top-label <i>number</i> preference <i>number</i>
Tree	static-entry
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

top-label *number*

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.
Context	network-instance name <i>string</i> mpls static-entry top-label number preference number
Range	16 to 1048575
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

preference *number*

Description	For a given top label value the entry with the lowest preference is selected as the active entry
Context	network-instance name <i>string</i> mpls static-entry top-label number preference number
Range	0 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

admin-state *keyword*

Description	Used to disable the entire static route and all its next-hops.
Context	network-instance name <i>string</i> mpls static-entry top-label number preference number admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

collect-stats *boolean*

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
Context	network-instance name <i>string</i> mpls static-entry top-label number preference number collect-stats boolean
Tree	collect-stats

Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

installed *boolean*

Description	Indicates whether the MPLS route entry was programmed in the data path.
Context	network-instance name <i>string</i> mpls static-entry top-label <i>number</i> preference <i>number</i> installed <i>boolean</i>
Tree	installed
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

next-hop-group *reference*

Description	Enter the next-hop-group context
Context	network-instance name <i>string</i> mpls static-entry top-label <i>number</i> preference <i>number</i> next-hop-group <i>reference</i>
Tree	next-hop-group
Reference	network-instance name <i>string</i> next-hop-groups <i>group name</i> <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

operation *keyword*

Description	The operation to be performed with the top label.
Context	network-instance name <i>string</i> mpls static-entry top-label <i>number</i> preference <i>number</i> operation <i>keyword</i>
Tree	operation
Default	swap
Options	<ul style="list-style-type: none"> • pop • swap
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

resolved-next-hop-group-id *reference*

Description	Enter the resolved-next-hop-group-id context
Context	network-instance name <i>string</i> mpls static-entry top-label <i>number</i> preference <i>number</i> resolved-next-hop-group-id <i>reference</i>
Tree	resolved-next-hop-group-id
Reference	network-instance name <i>string</i> route-table next-hop-group <i>index</i> <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

mpls-forwarding

Description	Enter the mpls-forwarding context
Context	network-instance name <i>string</i> mpls-forwarding
Tree	mpls-forwarding
Configurable	True
Platforms	Supported on all platforms

forward-received-packets *boolean*

Description	When set to true, MPLS packets received on any subinterface of the network-instance will be forwarded according to the matching ILM entries. When set to false, MPLS packets are discarded if received on any subinterface of the network-instance. In the default network-instance the default is 'true'.
Context	network-instance name <i>string</i> mpls-forwarding forward-received-packets <i>boolean</i>
Tree	forward-received-packets
Configurable	True
Platforms	Supported on all platforms

mtu

Description	Top-level container for configuration and state data related to network-instance MTU
Context	network-instance name <i>string</i> mtu
Tree	mtu
Configurable	True

Platforms Supported on all platforms

path-mtu-discovery *boolean*

Description Enables or disables path MTU discovery in this network-instance

This is controlled via the kernel `ip_no_pmtu_disc` 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.

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.

Context [network-instance name string mtu path-mtu-discovery boolean](#)

Tree [path-mtu-discovery](#)

Default true

Configurable True

Platforms Supported on all platforms

next-hop-groups

Description Enable the next-hop-groups context

Context [network-instance name string next-hop-groups](#)

Tree [next-hop-groups](#)

Configurable True

Platforms Supported on all platforms

group *name string*

Description Specifies the next hop group.

Context [network-instance name string next-hop-groups group name string](#)

Tree [group](#)

Configurable True

Platforms Supported on all platforms

name *string*

Description	Specifies the next hop group name
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Used to enable or disable a next-hop group
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

blackhole

Description	Enable the blackhole context
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> blackhole
Tree	blackhole
Configurable	True
Platforms	Supported on all platforms

generate-icmp *boolean*

Description	When set to true the router generates ICMP unreachable messages for the dropped packets
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> blackhole generate-icmp <i>boolean</i>
Tree	generate-icmp
Default	false
Configurable	True
Platforms	Supported on all platforms

nexthop *index number*

Description	Enter the nexthop list instance
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number
Tree	nexthop
Configurable	True
Platforms	Supported on all platforms
Max. Elements	128

index *number*

Description	Numerical index of the next-hop member
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Used to enable or disable a particular next-hop
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
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

failure-detection

Description	Enter the failure-detection context
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index number failure-detection
Tree	failure-detection
Configurable	True

Platforms Supported on all platforms

enable-bfd

Description Enable the enable-bfd context

Context [network-instance name string](#) [next-hop-groups group name string](#) [nexthop index number](#) [failure-detection enable-bfd](#)

Tree [enable-bfd](#)

Configurable True

Platforms Supported on all platforms

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

Description The local address to be used for the associated BFD session

Context [network-instance name string](#) [next-hop-groups group name string](#) [nexthop index number](#) [failure-detection enable-bfd local-address \(*ipv4-address | ipv6-address*\)](#)

Tree [local-address](#)

Configurable True

Platforms Supported on all platforms

local-discriminator *number*

Description The local discriminator to be used for the associated BFD session

Context [network-instance name string](#) [next-hop-groups group name string](#) [nexthop index number](#) [failure-detection enable-bfd local-discriminator *number*](#)

Tree [local-discriminator](#)

Range 1 to 16384

Configurable True

Platforms Supported on all platforms

remote-discriminator *number*

Description The remote discriminator to be used for the associated BFD session

Context [network-instance name string](#) [next-hop-groups group name string](#) [nexthop index number](#) [failure-detection enable-bfd remote-discriminator *number*](#)

Tree [remote-discriminator](#)

Range 1 to 16384

Configurable	True
Platforms	Supported on all platforms

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

Description	The next-hop IPv4 or IPv6 address
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index <i>number</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	ip-address
Configurable	True
Platforms	Supported on all platforms

pushed-mpls-label-stack (*number* | *keyword*)

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.
Context	network-instance name <i>string</i> next-hop-groups group name <i>string</i> nexthop index <i>number</i> pushed-mpls-label-stack (<i>number</i> <i>keyword</i>)
Tree	pushed-mpls-label-stack
Range	16 to 1048575
Options	<ul style="list-style-type: none"> • IPV4_EXPLICIT_NULL • IPV6_EXPLICIT_NULL • IMPLICIT_NULL
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6
Max. Elements	1

resolve *boolean*

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.
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

Default	true
Configurable	True
Platforms	Supported on all platforms

oper-mac-vrf-mtu *number*

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.
Context	network-instance name <i>string</i> oper-mac-vrf-mtu <i>number</i>
Tree	oper-mac-vrf-mtu
Range	1492 to 9500
Units	bytes
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	This leaf contains the operational state of the network instance.
Context	network-instance name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

policy-forwarding

Description

Configuration and operational state relating to policy-forwarding within a network instance.

Context[network-instance name](#) *string* [policy-forwarding](#)**Tree**[policy-forwarding](#)**Configurable**

True

Platforms

7250 IXR-10, 7250 IXR-6

interface [subinterface](#) *reference*

Description

List of subinterfaces that use the policy forwarding policy.

Context[network-instance name](#) *string* [policy-forwarding](#) [interface subinterface](#) *reference*

Tree	interface
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

subinterface *reference*

Description	A subinterface of the network-instance
Context	network-instance name <i>string</i> policy-forwarding interface subinterface reference
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

apply-forwarding-policy *reference*

Description	The policy to be applied on the interface. Packets ingress on the referenced interface should be compared to the match criteria within the specified policy, and in the case that these criteria are met, the forwarding actions specified applied.
Context	network-instance name <i>string</i> policy-forwarding interface subinterface reference apply-forwarding-policy reference
Tree	apply-forwarding-policy
Reference	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

policy [policy-id](#) *string*

Description	A forwarding policy is defined to have a set of match criteria, allowing particular fields of a packet's header to be matched, and a set of forwarding actions which determines how the local system should forward the packet.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i>
Tree	policy
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6
Max. Elements	4

policy-id *string*

Description	A unique name identifying the forwarding policy. This name is used when applying the policy to a particular interface.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

description *string*

Description	Description string for the policy
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

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

Description	List of policy forwarding rules.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i>
Tree	rule
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

sequence-id *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i>
Range	1 to 128
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

action

Description	Container for the actions to be applied to packets matching the policy forwarding rule.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> action
Tree	action
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

network-instance *reference*

Description	When this leaf is set, packets matching the match criteria for the forwarding rule should be looked up in the network-instance that is referenced rather than the network-instance with which the interface is associated.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> action network-instance <i>reference</i>
Tree	network-instance
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

description *string*

Description	Description string for the rule
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

match

Description	Container for the conditions that determine whether a packet matches this entry
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> match
Tree	match
Configurable	True

Platforms 7250 IXR-10, 7250 IXR-6

ipv4

Description Container for match conditions associated with IPv4 header fields
If no match conditions are provided then no IPv4 packets are matched.

Context [network-instance name](#) *string* [policy-forwarding policy](#) [policy-id](#) *string* [rule sequence-id](#) *number* [match ipv4](#)

Tree [ipv4](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

dscp-set (*number* | *keyword*)

Description A list of DSCP values to be matched for incoming packets. An OR match should be performed, such that a packet must match one of the values defined in this list. If the field is left empty then any DSCP value matches.

Context [network-instance name](#) *string* [policy-forwarding policy](#) [policy-id](#) *string* [rule sequence-id](#) *number* [match ipv4 dscp-set](#) (*number* | *keyword*)

Tree [dscp-set](#)

Range 0 to 63

Options

- CS0
- LE
- CS1
- AF11
- AF12
- AF13
- CS2
- AF21
- AF22
- AF23
- CS3
- AF31
- AF32
- AF33
- CS4
- AF41
- AF42

	<ul style="list-style-type: none"> • AF43 • CS5 • EF • CS6 • CS7
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

protocol (*number* | *keyword*)

Description	An IPv4 packet matches this condition if its IP protocol type field matches the specified value
Context	network-instance name string policy-forwarding policy policy-id string rule sequence-id number match ipv4 protocol (<i>number</i> <i>keyword</i>)
Tree	protocol
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
- ospf
OSPFv2 and OSPFv3
- 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
Platforms**

True
7250 IXR-10, 7250 IXR-6

source-ip

Description	Packet matching criteria based on source IPv4 address
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> match ipv4 source-ip
Tree	source-ip
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

prefix string

Description	Match a packet if its source IP address is within the specified IPv4 prefix.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> match ipv4 source-ip prefix <i>string</i>
Tree	prefix
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

tcam-entries number

Description	The number of TCAM entries required to implement this rule.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> rule sequence-id <i>number</i> tcam-entries <i>number</i>
Tree	tcam-entries
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

tcam-entries number

Description	The number of TCAM entries required to implement this entire policy.
Context	network-instance name <i>string</i> policy-forwarding policy policy-id <i>string</i> tcam-entries <i>number</i>
Tree	tcam-entries
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

protocols

Description	The routing protocols that are enabled for this network-instance.
--------------------	---

Context	network-instance name <i>string</i> protocols
Tree	protocols
Configurable	True
Platforms	Supported on all platforms

bgp

Description	Enable the bgp context
Context	network-instance name <i>string</i> protocols bgp
Tree	bgp
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

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.
Context	network-instance name <i>string</i> protocols bgp admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

as-path-options

Description	Options for handling the AS_PATH in received BGP routes
Context	network-instance name <i>string</i> protocols bgp as-path-options
Tree	as-path-options
Configurable	True
Platforms	Supported on all platforms

allow-own-as *number*

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
Context	network-instance name <i>string</i> protocols bgp as-path-options allow-own-as <i>number</i>
Tree	allow-own-as
Default	0
Configurable	True
Platforms	Supported on all platforms

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
Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as
Tree	remove-private-as
Configurable	True
Platforms	Supported on all platforms

ignore-peer-as *boolean*

Description	If set to true then do not delete or replace a private AS number that is the same as the peer AS number
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
Default	false
Configurable	True
Platforms	Supported on all platforms

leading-only *boolean*

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
Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as leading-only <i>boolean</i>

Tree	leading-only
Default	false
Configurable	True
Platforms	Supported on all platforms

mode *keyword*

Description	The method by which private AS numbers are removed from the advertised AS_PATH attribute
Context	network-instance name <i>string</i> protocols bgp as-path-options remove-private-as mode <i>keyword</i>
Tree	mode
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
Platforms	Supported on all platforms

authentication

Description	Container with authentication options that apply to all peers of the BGP instance
Context	network-instance name <i>string</i> protocols bgp authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Reference to a keychain. The keychain type must be tcp-md5.
Context	network-instance name <i>string</i> protocols bgp authentication keychain reference
Tree	keychain

Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

autonomous-system *number*

Description	The global AS number of the BGP instance Values greater than 65535 must be entered in ASPLAIN format.
Context	network-instance name <i>string</i> protocols bgp autonomous-system <i>number</i>
Tree	autonomous-system
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

convergence

Description	Options for configuring address family independent BGP convergence parameters
Context	network-instance name <i>string</i> protocols bgp convergence
Tree	convergence
Configurable	True
Platforms	Supported on all platforms

min-wait-to-advertise *number*

Description	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 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. This timer and associated state machine are only restarted by one of the following triggers:
Context	network-instance name <i>string</i> protocols bgp convergence min-wait-to-advertise <i>number</i>
Tree	min-wait-to-advertise
Range	0 to 3600

Default	0
Configurable	True
Platforms	Supported on all platforms

dynamic-neighbors

Description	Options related to the acceptance and initiation of dynamic BGP sessions
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors
Tree	dynamic-neighbors
Configurable	True
Platforms	Supported on all platforms

accept

Description	Options related to the acceptance of dynamic BGP sessions from remote peers
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept
Tree	accept
Configurable	True
Platforms	Supported on all platforms

match [prefix](#) (*ipv4-prefix | ipv6-prefix*)

Description	<p>List of prefix and group-id combinations from which incoming TCP connections to port 179 will be accepted</p> <p>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 source IP is not an IPv6 link-local address associated with an (unnumbered) interface configured for dynamic-neighbor sessions.</p>
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (<i>ipv4-prefix ipv6-prefix</i>)
Tree	match
Configurable	True
Platforms	Supported on all platforms

prefix (*ipv4-prefix | ipv6-prefix*)

Description	The IP prefix used to match an incoming dynamic BGP session to a group.
--------------------	---

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Configurable	True
Platforms	Supported on all platforms

allowed-peer-as *string*

Description	<p>The allowed AS numbers that can establish incoming BGP sessions from this prefix and group-id-range combination</p> <p>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</p>
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) allowed-peer-as <i>string</i>
Tree	allowed-peer-as
Configurable	True
Platforms	Supported on all platforms
Max. Elements	32

peer-group *reference*

Description	<p>Reference to a peer-group</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept match prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) peer-group <i>reference</i>
Tree	peer-group
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

max-sessions *number*

Description	<p>The maximum number of incoming BGP sessions that will be accepted by the router</p> <p>A value of 0 means no limit.</p>
--------------------	--

Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors accept max-sessions <i>number</i>
Tree	max-sessions
Default	0
Configurable	True
Platforms	Supported on all platforms

interface [interface-name](#) *reference*

Description	List of interfaces on which dynamic sessions based on IPv6 link-local address discovery are accepted and initiated.
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors interface interface-name <i>reference</i>
Tree	interface
Configurable	True
Platforms	Supported on all platforms

interface-name *reference*

Description	<p>Reference to a specific subinterface of the form <interface-name>.<subinterface-index></p> <p>The referenced subinterface should be enabled for IPv6 and should be configured to accept and send IPv6 router advertisement messages. The referenced subinterface does not need any IPv4 addresses or global-unicast IPv6 addresses (i.e. it can be an unnumbered interface).</p> <p>When a subinterface is present in this list, incoming TCP connections to the BGP well-known port that are received on this subinterface and sourced from an IPv6 link local address and destined for the IPv6 link local address of the subinterface are automatically accepted.</p> <p>When a subinterface is present in this list, received IPv6 router advertisement messages on this subinterface automatically trigger BGP session setup towards the sender of these messages, if there is not already an established session.</p>
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors interface interface-name <i>reference</i>
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

allowed-peer-as *string*

Description	Specifies the allowed AS numbers of dynamic BGP neighbors on this interface. If the OPEN message from a peer on this interface 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 string format as1..as2.
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors interface interface-name <i>reference</i> allowed-peer-as <i>string</i>
Tree	allowed-peer-as
Configurable	True
Platforms	Supported on all platforms
Max. Elements	32

peer-group *reference*

Description	Reference to a peer-group Specifies the peer-group to associate with dynamic BGP neighbors on this interface. The peer-group provides all the parameters needed to complete the establishment of the dynamic session.
Context	network-instance name <i>string</i> protocols bgp dynamic-neighbors interface interface-name <i>reference</i> peer-group <i>reference</i>
Tree	peer-group
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

ebgp-default-policy

Description	Options for controlling the default policies that apply to EBGp sessions
Context	network-instance name <i>string</i> protocols bgp ebgp-default-policy
Tree	ebgp-default-policy
Configurable	True
Platforms	Supported on all platforms

export-reject-all *boolean*

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
Context	network-instance name <i>string</i> protocols bgp ebgp-default-policy export-reject-all <i>boolean</i>

Tree	export-reject-all
Default	true
Configurable	True
Platforms	Supported on all platforms

import-reject-all *boolean*

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
Context	network-instance name <i>string</i> protocols bgp ebgp-default-policy import-reject-all <i>boolean</i>
Tree	import-reject-all
Default	true
Configurable	True
Platforms	Supported on all platforms

evpn

Description	Options related to the EVPN address family
Context	network-instance name <i>string</i> protocols bgp evpn
Tree	evpn
Configurable	True
Platforms	Supported on all platforms

active-routes *number*

Description	The total number of received EVPN routes that are currently installed in a mac-vrf and used for forwarding
Context	network-instance name <i>string</i> protocols bgp evpn active-routes <i>number</i>
Tree	active-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the EVPN address family on all sessions
--------------------	--

Context	network-instance name <i>string</i> protocols bgp evpn admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

advertise-ipv6-next-hops *boolean*

Description	<p>Enables advertisement of EVPN routes with IPv6 next-hops to peers</p> <p>If this is set to true and the local-address used towards the peer is an IPv6 address and BGP is supposed to apply next-hop-self then the route is advertised with the IPv6 local-address as the BGP next-hop. If this is set to false, then the EVPN route is advertised with an IPv4 next-hop.</p>
Context	network-instance name <i>string</i> protocols bgp evpn advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Default	false
Configurable	True
Platforms	Supported on all platforms

inter-as-vpn *boolean*

Description	<p>When set to true, received EVPN routes that are not imported by any network-instance are retained in the BGP RIB and considered 'used' so that they can be propagated to any EBGP or IBGP peer.</p> <p>This command supersedes the effect of keep-all-routes.</p>
Context	network-instance name <i>string</i> protocols bgp evpn inter-as-vpn <i>boolean</i>
Tree	inter-as-vpn
Default	false
Configurable	True
Platforms	Supported on all platforms

keep-all-routes *boolean*

Description	When this is set to true all received EVPN routes are retained in the RIB-IN, even those not imported by any network-instance; these routes display as 'rejected' and cannot be propagated to other peers. When this is false, EVPN routes that are not imported by any network-instance are dropped and not retained in the BGP RIB-IN; policy changes affecting received EVPN routes will trigger the sending of ROUTE_REFRESH messages towards all EVPN family peers.
Context	network-instance name <i>string</i> protocols bgp evpn keep-all-routes <i>boolean</i>
Tree	keep-all-routes
Default	false
Configurable	True
Platforms	Supported on all platforms

rapid-update *boolean*

Description	When this is set to true, EVPN UPDATEs advertising reachability and withdrawals are advertised immediately, bypassing the session level min-route-advertisement-interval. When this is false, reachability updates and withdrawals are subject to the MRAI interval.
Context	network-instance name <i>string</i> protocols bgp evpn rapid-update <i>boolean</i>
Tree	rapid-update
Default	false
Configurable	True
Platforms	Supported on all platforms

received-routes *number*

Description	The total number of EVPN routes received from all peers of the BGP instance
Context	network-instance name <i>string</i> protocols bgp evpn received-routes <i>number</i>
Tree	received-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

export-policy *reference*

Description	Apply an export policy to advertised BGP routes
--------------------	---

Context	network-instance name <i>string</i> protocols bgp export-policy <i>reference</i>
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

failure-detection

Description	Options related to methods of detecting BGP session failure
Context	network-instance name <i>string</i> protocols bgp failure-detection
Tree	failure-detection
Configurable	True
Platforms	Supported on all platforms

enable-bfd *boolean*

Description	The true setting enables Bi-directional Forwarding Detection on BGP sessions belonging to the peer group
Context	network-instance name <i>string</i> protocols bgp failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Default	false
Configurable	True
Platforms	Supported on all platforms

fast-failover *boolean*

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
Context	network-instance name <i>string</i> protocols bgp failure-detection fast-failover <i>boolean</i>
Tree	fast-failover
Default	true
Configurable	True
Platforms	Supported on all platforms

graceful-restart

Description	Options for controlling the behavior of the router as a graceful restart helper
Context	network-instance name <i>string</i> protocols bgp graceful-restart
Tree	graceful-restart
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable graceful restart helper for all address families
Context	network-instance name <i>string</i> protocols bgp graceful-restart admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

stale-routes-time *number*

Description	<p>The maximum number of seconds that routes received from a helped peer remain stale until they are deleted</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp graceful-restart stale-routes-time number
Tree	stale-routes-time
Range	1 to 3600
Default	360
Units	seconds
Configurable	True
Platforms	Supported on all platforms

group *group-name string*

Description	Peer group templates
Context	network-instance name string protocols bgp group group-name string
Tree	group
Configurable	True
Platforms	Supported on all platforms

group-name *string*

Description	The configured name of the peer group
Context	network-instance name string protocols bgp group group-name string
String Length	1 to 64
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

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.
Context	network-instance name string protocols bgp group group-name string admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

as-path-options

Description	Options for handling the AS_PATH in received BGP routes
Context	network-instance name string protocols bgp group group-name string as-path-options
Tree	as-path-options
Configurable	True
Platforms	Supported on all platforms

allow-own-as *number*

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.
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
Configurable	True
Platforms	Supported on all platforms

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
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
Configurable	True
Platforms	Supported on all platforms

ignore-peer-as *boolean*

Description	If set to true then do not delete or replace a private AS number that is the same as the peer AS number
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
Default	false
Configurable	True
Platforms	Supported on all platforms

leading-only *boolean*

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
--------------------	---

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
Default	false
Configurable	True
Platforms	Supported on all platforms

mode *keyword*

Description	The method by which private AS numbers are removed from the advertised AS_PATH attribute
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
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
Platforms	Supported on all platforms

replace-peer-as *boolean*

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
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> as-path-options replace-peer-as <i>boolean</i>
Tree	replace-peer-as
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container with authentication options that apply to all peers in this peer-group
--------------------	--

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Reference to a keychain. The keychain type must be tcp-md5.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> authentication keychain <i>reference</i>
Tree	keychain
Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	A user provided description string for the peer group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

evpn

Description	Options related to the EVPN address family
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> evpn
Tree	evpn
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the EVPN address family on the BGP sessions of the peer-group
--------------------	--

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> evpn admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

advertise-ipv6-next-hops *boolean*

Description	<p>Enables advertisement of EVPN routes with IPv6 next-hops to peers in the peer-group</p> <p>If this is set to true and the local-address used towards the peer is an IPv6 address and BGP is supposed to apply next-hop-self then the route is advertised with the IPv6 local-address as the BGP next-hop. If this is set to false, then the EVPN route is advertised with an IPv4 next-hop.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> evpn advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Configurable	True
Platforms	Supported on all platforms

prefix-limit

Description	Options for configuring the maximum number of EVPN routes allowed to be received from each peer in the peer-group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> evpn prefix-limit
Tree	prefix-limit
Configurable	True
Platforms	Supported on all platforms

max-received-routes *number*

Description	Maximum number of EVPN routes that will be accepted from each neighbor, counting routes accepted and rejected by import policies
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> evpn prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes

Range	1 to 4294967295
Default	4294967295
Configurable	True
Platforms	Supported on all platforms

warning-threshold-pct *number*

Description	When the number of EVPN 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
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> evpn prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

export-policy *reference*

Description	Apply an export policy to advertised BGP routes
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> export-policy <i>reference</i>
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

failure-detection

Description	Options related to methods of detecting BGP session failure
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> failure-detection
Tree	failure-detection
Configurable	True
Platforms	Supported on all platforms

enable-bfd *boolean*

Description	The true setting enables Bi-directional Forwarding Detection on BGP sessions belonging to the peer group
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
Configurable	True
Platforms	Supported on all platforms

fast-failover *boolean*

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
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
Configurable	True
Platforms	Supported on all platforms

graceful-restart

Description	Options related to router behavior as a graceful restart helper
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> graceful-restart
Tree	graceful-restart
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable graceful restart helper for all address families
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
Options	<ul style="list-style-type: none"> • enable • disable

Configurable	True
Platforms	Supported on all platforms

stale-routes-time *number*

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.
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
Range	1 to 3600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

import-policy *reference*

Description	Apply an import policy to received BGP routes
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> import-policy reference
Tree	import-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

ipv4-unicast

Description	Options related to the IPv4-unicast address family
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast
Tree	ipv4-unicast
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the IPv4 unicast address family on all sessions belonging to the group
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
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

advertise-ipv6-next-hops *boolean*

Description	<p>Enables advertisement of IPv4 routes with IPv6 next-hops to peers in the group</p> <p>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).</p>
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
Configurable	True
Platforms	Supported on all platforms

prefix-limit

Description	Options for configuring the maximum number of IPv4 routes allowed to be received from each peer in the group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv4-unicast prefix-limit
Tree	prefix-limit
Configurable	True
Platforms	Supported on all platforms

max-received-routes *number*

Description	Maximum number of IPv4 routes that will be accepted from each neighbor, counting routes accepted and rejected by import policies
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
Range	1 to 4294967295
Default	4294967295
Configurable	True
Platforms	Supported on all platforms

warning-threshold-pct *number*

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
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
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

receive-ipv6-next-hops *boolean*

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.
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
Configurable	True
Platforms	Supported on all platforms

ipv6-unicast

Description	Options related to the IPv6-unicast address family
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast
Tree	ipv6-unicast
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the IPv6 unicast address family on all sessions belonging to the group
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
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

prefix-limit

Description	Options for configuring the maximum number of IPv6 routes allowed to be received from each peer in the group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> ipv6-unicast prefix-limit
Tree	prefix-limit
Configurable	True
Platforms	Supported on all platforms

max-received-routes *number*

Description	Maximum number of IPv6 routes that will be accepted from each neighbor, counting routes accepted and rejected by import policies
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
Range	1 to 4294967295

Default	4294967295
Configurable	True
Platforms	Supported on all platforms

warning-threshold-pct *number*

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
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
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

local-as [as-number](#) *number*

Description	Options related to the local autonomous-system number advertised by this router to its peers
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
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

as-number *number*

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.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> local-as as-number <i>number</i>
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

prepend-global-as *boolean*

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.
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
Default	true
Configurable	True
Platforms	Supported on all platforms

prepend-local-as *boolean*

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
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> local-as as-number <i>number</i> prepend-local-as <i>boolean</i>
Tree	prepend-local-as
Default	true
Configurable	True
Platforms	Supported on all platforms

local-preference *number*

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.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> local-preference <i>number</i>
Tree	local-preference
Configurable	True
Platforms	Supported on all platforms

maintenance-group *string*

Description	State field to display the maintenance group to which this group belongs to.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> maintenance-group <i>string</i>
Tree	maintenance-group
Configurable	False
Platforms	Supported on all platforms

multihop

Description	Configuration parameters specifying the multihop behaviour for EBGp peers in the peer group.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> multihop
Tree	multihop
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	<p>When enabled, IBGP and EBGp peers in the group are allowed to be indirectly connected by up to N hops, where N is controlled by the maximum-hops parameter. When disabled, only IBGP peers within the peer group support multihop.</p> <p>This can be overridden on a per neighbor basis. It is inherited by neighbors in the peer-group only if maximum-hops is also specified.</p> <p>By default this is disabled.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> multihop admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

maximum-hops *number*

Description	This sets the maximum number of routing hops towards each peer. It determines the IP TTL value in originated BGP TCP/IP packets. By default
--------------------	---

the TTL is set to 1 towards EBGP peers and 64 towards IBGP peers. This leaf sets a new IP TTL to use towards both EBGP and IBGP peers in the peer group.

This can be overridden on a per neighbor basis. It is inherited by neighbors in the peer-group only if admin-state is also specified.

Context	<code>network-instance name string protocols bgp group group-name string multihop maximum-hops number</code>
Tree	<code>maximum-hops</code>
Range	1 to 255
Configurable	True
Platforms	Supported on all platforms

next-hop-self *boolean*

Description	When set to true, the next-hop in all IPv4-unicast, IPv6-unicast and EVPN BGP routes advertised to all IBGP peers in the peer-group is set equal to the local-address used on each 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-client, IBGP-non-client or redistributed direct/static/aggregate route). When set to false, normal BGP rules from RFC 4271 apply.
Context	<code>network-instance name string protocols bgp group group-name string next-hop-self boolean</code>
Tree	<code>next-hop-self</code>
Default	false
Configurable	True
Platforms	Supported on all platforms

peer-as *number*

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.
Context	<code>network-instance name string protocols bgp group group-name string peer-as number</code>
Tree	<code>peer-as</code>
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

route-reflector

Description	Container with route reflection configuration options.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> route-reflector
Tree	route-reflector
Configurable	True
Platforms	Supported on all platforms

client *boolean*

Description	When this is set to true all configured and dynamic BGP sessions that belong to the peer-group are considered RR clients.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> route-reflector client <i>boolean</i>
Tree	client
Configurable	True
Platforms	Supported on all platforms

cluster-id *string*

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.
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
Configurable	True
Platforms	Supported on all platforms

send-community

Description	Options for controlling the sending of BGP communities to peers in the group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-community
Tree	send-community
Configurable	True
Platforms	Supported on all platforms

large *boolean*

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
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-community large <i>boolean</i>
Tree	large
Configurable	True
Platforms	Supported on all platforms

standard *boolean*

Description	The false setting causes BGP to strip all standard (4 byte) communities from all outbound routes advertised to each peer in the group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-community standard <i>boolean</i>
Tree	standard
Configurable	True
Platforms	Supported on all platforms

send-default-route

Description	Options for controlling the generation of default routes towards group peers
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> send-default-route
Tree	send-default-route
Configurable	True
Platforms	Supported on all platforms

export-policy *reference*

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.
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
Reference	routing-policy policy name <i>string</i>

Configurable	True
Platforms	Supported on all platforms

ipv4-unicast *boolean*

Description	Enables the sending of a synthetically generated default IPv4 route [0/0] to each peer in the group
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
Default	false
Configurable	True
Platforms	Supported on all platforms

ipv6-unicast *boolean*

Description	Enables the sending of a synthetically generated default IPv6 route [::/0] to each peer in the group
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
Default	false
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Container for BGP statistics.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

disabled-peers *number*

Description	The number of configured BGP peers associated with the peer-group that are administratively disabled
--------------------	--

Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics disabled-peers <i>number</i>
Tree	disabled-peers
Configurable	False
Platforms	Supported on all platforms

dynamic-peers *number*

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
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics dynamic-peers <i>number</i>
Tree	dynamic-peers
Configurable	False
Platforms	Supported on all platforms

path-memory *number*

Description	The total number of bytes required to store the path attribute objects used by received BGP routes associated with the peer-group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics path-memory <i>number</i>
Tree	path-memory
Default	0
Configurable	False
Platforms	Supported on all platforms

total-active-routes *number*

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
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
Default	0
Configurable	False

Platforms Supported on all platforms

total-paths *number*

Description The total number of path attribute objects used by received BGP routes associated with the peer-group

Context [network-instance name](#) *string* [protocols bgp group group-name](#) *string* [statistics total-paths](#) *number*

Tree [total-paths](#)

Default 0

Configurable False

Platforms Supported on all platforms

total-peers *number*

Description The total number of configured BGP peers associated with the peer-group

Context [network-instance name](#) *string* [protocols bgp group group-name](#) *string* [statistics total-peers](#) *number*

Tree [total-peers](#)

Configurable False

Platforms Supported on all platforms

total-prefixes *number*

Description The total number of unique NLRI contained in all received BGP routes associated with the BGP instance or the peer-group.

Context [network-instance name](#) *string* [protocols bgp group group-name](#) *string* [statistics total-prefixes](#) *number*

Tree [total-prefixes](#)

Configurable False

Platforms Supported on all platforms

total-received-routes *number*

Description The total number of received BGP routes associated with the peer-group, summed across all address families

Context [network-instance name](#) *string* [protocols bgp group group-name](#) *string* [statistics total-received-routes](#) *number*

Tree [total-received-routes](#)

Default	0
Configurable	False
Platforms	Supported on all platforms

up-peers *number*

Description	The number of configured BGP peers associated with the peer-group that are currently in the established state
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> statistics up-peers <i>number</i>
Tree	up-peers
Configurable	False
Platforms	Supported on all platforms

timers

Description	Enter the timers context
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers
Tree	timers
Configurable	True
Platforms	Supported on all platforms

connect-retry *number*

Description	The time interval in seconds between successive attempts to establish a session with a peer
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers connect-retry <i>number</i>
Tree	connect-retry
Range	1 to 65535
Default	120
Units	seconds
Configurable	True
Platforms	Supported on all platforms

hold-time *number*

Description	<p>The hold-time interval in seconds that the router proposes to the peer in its OPEN message</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers hold-time <i>number</i>
Tree	hold-time
Range	0 3 to 65535
Default	90
Units	seconds
Configurable	True
Platforms	Supported on all platforms

keepalive-interval *number*

Description	<p>The interval in seconds between successive keepalive messages sent to the peer</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> timers keepalive-interval <i>number</i>
Tree	keepalive-interval
Range	0 to 21845
Units	seconds
Configurable	True
Platforms	Supported on all platforms

minimum-advertisement-interval *number*

Description	<p>The value assigned to the MinRouteAdvertisementIntervalTimer of RFC 4271, for both EBGp and IBGP sessions</p> <p>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.</p>
--------------------	---

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
Range	1 to 255
Default	5
Units	seconds
Configurable	True
Platforms	Supported on all platforms

trace-options

Description	Debug traceoptions for BGP
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

flag [name](#) *keyword*

Description	Tracing parameters
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options flag name <i>keyword</i>
Tree	flag
Configurable	True
Platforms	Supported on all platforms

name *keyword*

Description	Enter the name context
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> trace-options flag name <i>keyword</i>
Options	<ul style="list-style-type: none"> • <code>events</code> Trace all BGP events. • <code>packets</code> Trace all BGP protocol packets. • <code>open</code> 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
Platforms	Supported on all platforms

modifier *keyword*

Description	Enter the modifier context
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
Options	<ul style="list-style-type: none"> • <code>detail</code> To enable detailed tracing. Includes both received and sent packets. • <code>receive</code> To enable tracing for the packets which are received. • <code>send</code> To enable tracing for the sent packets.
Configurable	True
Platforms	Supported on all platforms

transport

Description	Enter the transport context
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> transport

Tree	transport
Configurable	True
Platforms	Supported on all platforms

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

Description	<p>The local TCP endpoint of used for all BGP sessions in the group</p> <p>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.</p> <p>This address must be the primary address of an interface, otherwise the session will not come up.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> transport local-address (<i>ipv4-address</i> <i>ipv6-address</i> <i>string</i>)
Tree	local-address
Configurable	True
Platforms	Supported on all platforms

passive-mode *boolean*

Description	<p>The true setting causes BGP to wait for the peer to initiate the TCP connection</p> <p>The false setting causes BGP to initiate a TCP connection whenever the BGP session is started or restarted.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> transport passive-mode <i>boolean</i>
Tree	passive-mode
Default	false
Configurable	True
Platforms	Supported on all platforms

tcp-mss *number*

Description	<p>The maximum segment size for each BGP TCP session belonging to the group</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> transport tcp-mss <i>number</i>
Tree	tcp-mss

Range	536 to 9446
Units	bytes
Configurable	True
Platforms	Supported on all platforms

under-maintenance *boolean*

Description	State field to determine if this bgp group is in maintenance mode.
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> under-maintenance <i>boolean</i>
Tree	under-maintenance
Configurable	False
Platforms	Supported on all platforms

import-policy *reference*

Description	Apply an import policy to received BGP routes
Context	network-instance name <i>string</i> protocols bgp import-policy <i>reference</i>
Tree	import-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

ipv4-unicast

Description	Options related to the IPv4-unicast address family
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast
Tree	ipv4-unicast
Configurable	True
Platforms	Supported on all platforms

active-routes *number*

Description	The total number of received IPv4 unicast routes that are currently used for forwarding
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast active-routes <i>number</i>

Tree	active-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the IPv4 unicast address family on all sessions
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

advertise-ipv6-next-hops *boolean*

Description	<p>Enables advertisement of IPv4 routes with IPv6 next-hops to peers</p> <p>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).</p>
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Default	false
Configurable	True
Platforms	Supported on all platforms

convergence

Description	Options for controlling and monitoring routing convergence of the relevant address family
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence

Tree	convergence
Configurable	True
Platforms	Supported on all platforms

converged-peers *number*

Description	The number of peers that have sent an EOR marker for the address family since the last BGP restart
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence converged-peers <i>number</i>
Tree	converged-peers
Configurable	False
Platforms	Supported on all platforms

convergence-state *keyword*

Description	Enter the convergence-state context
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence convergence-state <i>keyword</i>
Tree	convergence-state
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
Platforms	Supported on all platforms

convergence-time *number*

Description	The elapsed time in seconds, starting from the last BGP restart, to reach the converged state for the address family
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence convergence-time <i>number</i>
Tree	convergence-time
Configurable	False
Platforms	Supported on all platforms

first-up-peer-time *number*

Description	The time when the first session supporting the address family came up, measured from the time that the BGP instance restarted
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence first-up-peer-time <i>number</i>
Tree	first-up-peer-time
Configurable	False
Platforms	Supported on all platforms

last-up-peer-time *number*

Description	The time when the last session supporting the address family came up, measured from the time that the BGP instance restarted
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence last-up-peer-time <i>number</i>
Tree	last-up-peer-time
Configurable	False
Platforms	Supported on all platforms

max-wait-to-advertise *number*

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>
--------------------	--

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence max-wait-to-advertise <i>number</i>
Tree	max-wait-to-advertise
Range	0 to 3600
Default	0
Configurable	True
Platforms	Supported on all platforms

oper-max-wait-to-advertise *number*

Description	The operational value of the max-wait-to-advertise timer for the address family
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
Range	0 to 10800
Configurable	False
Platforms	Supported on all platforms

up-peers *number*

Description	The number of BGP sessions (configured and dynamic) that support the address family and that are currently in the established state
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast convergence up-peers <i>number</i>
Tree	up-peers
Configurable	False
Platforms	Supported on all platforms

up-peers-when-min-expired *number*

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
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
Configurable	False
Platforms	Supported on all platforms

multipath

Description	Options related to BGP multipath
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath
Tree	multipath
Configurable	True
Platforms	Supported on all platforms

allow-multiple-as *boolean*

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
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath allow-multiple-as <i>boolean</i>
Tree	allow-multiple-as
Default	true
Configurable	True
Platforms	Supported on all platforms

max-paths-level-1 *number*

Description	The maximum number of BGP ECMP next-hops for BGP routes with an NLRI belonging to the address family of this configuration context
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath max-paths-level-1 <i>number</i>
Tree	max-paths-level-1
Range	1 to 64
Default	1
Configurable	True
Platforms	Supported on all platforms

max-paths-level-2 *number*

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
--------------------	---

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast multipath max-paths-level-2 <i>number</i>
Tree	max-paths-level-2
Range	1 to 64
Default	1
Configurable	True
Platforms	Supported on all platforms

next-hop-resolution

Description	Options for controlling next-hop resolution procedures
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast next-hop-resolution
Tree	next-hop-resolution
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-next-hops

Description	Options related to the resolution of BGP next-hops that are IPv4 addresses
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast next-hop-resolution ipv4-next-hops
Tree	ipv4-next-hops
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

tunnel-resolution

Description	Options related to resolution using tunnels in the tunnel table
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast next-hop-resolution ipv4-next-hops tunnel-resolution
Tree	tunnel-resolution
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

allowed-tunnel-types *identityref*

Description	List of allowed tunnel types
--------------------	------------------------------

Context	network-instance name <i>string</i> protocols bgp ipv4-unicast next-hop-resolution ipv4-next-hops tunnel-resolution allowed-tunnel-types identityref
Tree	allowed-tunnel-types
Options	<ul style="list-style-type: none"> • <code>sr-isis</code> Segment routing using MPLS dataplane, programmed by IS-IS • <code>sr-ospfv2</code> Segment routing using MPLS dataplane, programmed by OSPFv2 • <code>sr-ospfv3</code> Segment routing using MPLS dataplane, programmed by OSPFv3 • <code>vxlan</code> Tunnels based on VXLAN encapsulation
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

mode *keyword*

Description	Mode to control the order of tunnel resolution compared to route resolution
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast next-hop-resolution ipv4-next-hops tunnel-resolution mode <i>keyword</i>
Tree	mode
Default	disabled
Options	<ul style="list-style-type: none"> • <code>prefer</code> • <code>require</code> • <code>disabled</code>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

receive-ipv6-next-hops *boolean*

Description	<p>Enables the advertisement of the RFC 5549 capability to receive IPv4 routes with IPv6 next-hops</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast receive-ipv6-next-hops <i>boolean</i>

Tree	receive-ipv6-next-hops
Default	false
Configurable	True
Platforms	Supported on all platforms

received-routes *number*

Description	The total number of IPv4 unicast routes received from all peers of the BGP instance
Context	network-instance name <i>string</i> protocols bgp ipv4-unicast received-routes number
Tree	received-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

ipv6-unicast

Description	Options related to the IPv6-unicast address family
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast
Tree	ipv6-unicast
Configurable	True
Platforms	Supported on all platforms

active-routes *number*

Description	The total number of received IPv6 unicast routes that are currently used for forwarding
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast active-routes number
Tree	active-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the IPv6 unicast address family on all sessions
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

convergence

Description	Options for controlling and monitoring routing convergence of the relevant address family
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence
Tree	convergence
Configurable	True
Platforms	Supported on all platforms

converged-peers *number*

Description	The number of peers that have sent an EOR marker for the address family since the last BGP restart
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence converged-peers <i>number</i>
Tree	converged-peers
Configurable	False
Platforms	Supported on all platforms

convergence-state *keyword*

Description	Enter the convergence-state context
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence convergence-state <i>keyword</i>
Tree	convergence-state
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 advertised the End-of-RIB marker for the address family

Configurable	False
Platforms	Supported on all platforms

convergence-time *number*

Description	The elapsed time in seconds, starting from the last BGP restart, to reach the converged state for the address family
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence convergence-time <i>number</i>
Tree	convergence-time
Configurable	False
Platforms	Supported on all platforms

first-up-peer-time *number*

Description	The time when the first session supporting the address family came up, measured from the time that the BGP instance restarted
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence first-up-peer-time <i>number</i>
Tree	first-up-peer-time
Configurable	False
Platforms	Supported on all platforms

last-up-peer-time *number*

Description	The time when the last session supporting the address family came up, measured from the time that the BGP instance restarted
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence last-up-peer-time <i>number</i>
Tree	last-up-peer-time
Configurable	False
Platforms	Supported on all platforms

max-wait-to-advertise *number*

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>
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence max-wait-to-advertise <i>number</i>
Tree	max-wait-to-advertise
Range	0 to 3600
Default	0
Configurable	True
Platforms	Supported on all platforms

oper-max-wait-to-advertise *number*

Description	The operational value of the max-wait-to-advertise timer for the address family
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
Range	0 to 10800
Configurable	False
Platforms	Supported on all platforms

up-peers *number*

Description	The number of BGP sessions (configured and dynamic) that support the address family and that are currently in the established state
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast convergence up-peers <i>number</i>
Tree	up-peers
Configurable	False
Platforms	Supported on all platforms

up-peers-when-min-expired *number*

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
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
Configurable	False
Platforms	Supported on all platforms

multipath

Description	Options related to BGP multipath
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath
Tree	multipath
Configurable	True
Platforms	Supported on all platforms

allow-multiple-as *boolean*

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
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath allow-multiple-as <i>boolean</i>
Tree	allow-multiple-as
Default	true

Configurable	True
Platforms	Supported on all platforms

max-paths-level-1 *number*

Description	The maximum number of BGP ECMP next-hops for BGP routes with an NLRI belonging to the address family of this configuration context
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath max-paths-level-1 <i>number</i>
Tree	max-paths-level-1
Range	1 to 64
Default	1
Configurable	True
Platforms	Supported on all platforms

max-paths-level-2 *number*

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
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast multipath max-paths-level-2 <i>number</i>
Tree	max-paths-level-2
Range	1 to 64
Default	1
Configurable	True
Platforms	Supported on all platforms

next-hop-resolution

Description	Options for controlling next-hop resolution procedures
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast next-hop-resolution
Tree	next-hop-resolution
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-next-hops

Description	Options related to the resolution of BGP next-hops that are IPv4 addresses
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast next-hop-resolution ipv4-next-hops
Tree	ipv4-next-hops
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

tunnel-resolution

Description	Options related to resolution using tunnels in the tunnel table
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast next-hop-resolution ipv4-next-hops tunnel-resolution
Tree	tunnel-resolution
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

allowed-tunnel-types *identityref*

Description	List of allowed tunnel types
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast next-hop-resolution ipv4-next-hops tunnel-resolution allowed-tunnel-types <i>identityref</i>
Tree	allowed-tunnel-types
Options	<ul style="list-style-type: none"> • <code>sr-isis</code> Segment routing using MPLS dataplane, programmed by IS-IS • <code>sr-ospfv2</code> Segment routing using MPLS dataplane, programmed by OSPFv2 • <code>sr-ospfv3</code> Segment routing using MPLS dataplane, programmed by OSPFv3 • <code>vxlan</code> Tunnels based on VXLAN encapsulation
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

mode *keyword*

Description	Mode to control the order of tunnel resolution compared to route resolution
--------------------	---

Context	network-instance name <i>string</i> protocols bgp ipv6-unicast next-hop-resolution ipv4-next-hops tunnel-resolution mode <i>keyword</i>
Tree	mode
Default	disabled
Options	<ul style="list-style-type: none"> • prefer • require • disabled
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

received-routes *number*

Description	The total number of IPv6 unicast routes received from all peers of the BGP instance
Context	network-instance name <i>string</i> protocols bgp ipv6-unicast received-routes <i>number</i>
Tree	received-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

local-preference *number*

Description	<p>The value of the local-preference attribute that is added to received routes from EBGPeers</p> <p>It is also used to encode the local preference attribute for locally generated BGP routes.</p>
Context	network-instance name <i>string</i> protocols bgp local-preference <i>number</i>
Tree	local-preference
Default	100
Configurable	True
Platforms	Supported on all platforms

maintenance-group *string*

Description	State field to display the maintenance group to which this bgp instance belongs to.
Context	network-instance name <i>string</i> protocols bgp maintenance-group <i>string</i>

Tree	maintenance-group
Configurable	False
Platforms	Supported on all platforms

neighbor [peer-address](#) (*ipv4-address* | *ipv6-address-with-zone*)

Description	Create a configured BGP session
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Tree	neighbor
Configurable	True
Platforms	Supported on all platforms

peer-address (*ipv4-address* | *ipv6-address-with-zone*)

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the peer Disable will tear down the BGP session (return it to IDLE state).
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

advertised-capabilities *keyword*

Description	List of BGP capabilities advertised by the local routing device to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) advertised-capabilities keyword
Tree	advertised-capabilities
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
Platforms	Supported on all platforms

as-path-options

Description	Options for handling the AS_PATH in received BGP routes
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) as-path-options
Tree	as-path-options
Configurable	True
Platforms	Supported on all platforms

allow-own-as *number*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) as-path-options allow-own-as number
Tree	allow-own-as
Configurable	True
Platforms	Supported on all platforms

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) as-path-options remove-private-as
Tree	remove-private-as
Configurable	True
Platforms	Supported on all platforms

ignore-peer-as *boolean*

Description	If set to true then do not delete or replace a private AS number that is the same as the peer AS number
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) as-path-options remove-private-as ignore-peer-as <i>boolean</i>
Tree	ignore-peer-as
Default	false
Configurable	True
Platforms	Supported on all platforms

leading-only *boolean*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) as-path-options remove-private-as leading-only <i>boolean</i>
Tree	leading-only
Default	false
Configurable	True
Platforms	Supported on all platforms

mode *keyword*

Description	The method by which private AS numbers are removed from the advertised AS_PATH attribute
--------------------	--

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) as-path-options remove-private-as <i>mode keyword</i>
Tree	mode
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
Platforms	Supported on all platforms

replace-peer-as *boolean*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) as-path-options replace-peer-as <i>boolean</i>
Tree	replace-peer-as
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container with authentication options that apply to this specific peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Reference to a keychain. The keychain type must be tcp-md5.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) authentication keychain <i>reference</i>

Tree	keychain
Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

transmit-active *boolean*

Description	Reads true when the TCP segments being sent to the peer have authentication data.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) authentication transmit-active <i>boolean</i>
Tree	transmit-active
Configurable	False
Platforms	Supported on all platforms

description *string*

Description	A user provided description string for the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

discovered-by-lldp *boolean*

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)
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) discovered-by-lldp <i>boolean</i>
Tree	discovered-by-lldp
Configurable	False
Platforms	Supported on all platforms

dynamic-neighbor *boolean*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) dynamic-neighbor <i>boolean</i>
Tree	dynamic-neighbor
Configurable	False
Platforms	Supported on all platforms

established-transitions *number*

Description	The total number of times the BGP FSM transitioned into the established state for this peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) established-transitions <i>number</i>
Tree	established-transitions
Default	0
Configurable	False
Platforms	Supported on all platforms

evpn

Description	Options related to the EVPN address family
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) evpn
Tree	evpn
Configurable	True
Platforms	Supported on all platforms

active-routes *number*

Description	The number of EVPN routes received from the peer that are currently used for forwarding
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) evpn active-routes <i>number</i>
Tree	active-routes
Configurable	False
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the EVPN address family on the BGP session
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) evpn admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

advertise-ipv6-next-hops *boolean*

Description	<p>Enables advertisement of EVPN routes with IPv6 next-hops to peers</p> <p>If this is set to true and the local-address used towards the peer is an IPv6 address and BGP is supposed to apply next-hop-self then the route is advertised with the IPv6 local-address as the BGP next-hop. If this is set to false, then the EVPN route is advertised with an IPv4 next-hop.</p>
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) evpn advertise-ipv6-next-hops <i>boolean</i>
Tree	advertise-ipv6-next-hops
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Enter the oper-state context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) evpn oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up Negotiated operational state of the EVPN address family is up • down Negotiated operational state of the EVPN address family is down
Configurable	False
Platforms	Supported on all platforms

prefix-limit

Description	Options for configuring the maximum number of EVPN routes allowed to be received from the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) evpn prefix-limit
Tree	prefix-limit
Configurable	True
Platforms	Supported on all platforms

max-received-routes *number*

Description	Maximum number of EVPN routes that will be accepted from the neighbor, counting routes accepted and rejected by import policies
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) evpn prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

warning-threshold-pct *number*

Description	When the number of EVPN 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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) evpn prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Range	0 to 100
Configurable	True
Platforms	Supported on all platforms

received-routes *number*

Description	The number of EVPN routes received from the peer, including routes rejected by import policy
--------------------	--

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) evpn received-routes <i>number</i>
Tree	received-routes
Configurable	False
Platforms	Supported on all platforms

rejected-routes *number*

Description	The number of EVPN routes received from the peer that were rejected by import policy
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) evpn rejected-routes <i>number</i>
Tree	rejected-routes
Configurable	False
Platforms	Supported on all platforms

sent-routes *number*

Description	The number of EVPN routes advertised as reachable to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) evpn sent-routes <i>number</i>
Tree	sent-routes
Configurable	False
Platforms	Supported on all platforms

export-policy *reference*

Description	Apply an export policy to advertised BGP routes
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) export-policy <i>reference</i>
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

failure-detection

Description	Options related to methods of detecting BGP session failure
--------------------	---

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) failure-detection
Tree	failure-detection
Configurable	True
Platforms	Supported on all platforms

enable-bfd *boolean*

Description	The true setting enables Bi-directional Forwarding Detection on BGP sessions belonging to the peer group
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Configurable	True
Platforms	Supported on all platforms

fast-failover *boolean*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) failure-detection fast-failover <i>boolean</i>
Tree	fast-failover
Configurable	True
Platforms	Supported on all platforms

graceful-restart

Description	Options related to router behavior as a graceful restart helper
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart
Tree	graceful-restart
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable graceful restart helper for all address families
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart admin-state keyword
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

helper-active *boolean*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart helper-active boolean
Tree	helper-active
Configurable	False
Platforms	Supported on all platforms

last-restart-time *string*

Description	The last time the peer restarted
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart last-restart-time string
Tree	last-restart-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-capability

Description	Container for information about the last GR capability received from the neighbor
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart neighbor-capability

Tree	neighbor-capability
Configurable	False
Platforms	Supported on all platforms

afi-safi *name keyword*

Description	List of AFI/SAFI TLVs that were contained in the neighbor's last GR capability
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) graceful-restart neighbor-capability afi-safi name keyword
Tree	afi-safi
Configurable	False
Platforms	Supported on all platforms

name *keyword*

Description	Enter the name context
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) graceful-restart neighbor-capability afi-safi name keyword
Options	<ul style="list-style-type: none"> • ipv4-unicast • ipv6-unicast
Configurable	False
Platforms	Supported on all platforms

forwarding-preserved *boolean*

Description	The F-bit setting in the AFI/SAFI TLV
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) graceful-restart neighbor-capability afi-safi name keyword forwarding-preserved boolean
Tree	forwarding-preserved
Configurable	False
Platforms	Supported on all platforms

restart-time *number*

Description	The value of the Restart Time in the neighbor's last GR capability
--------------------	--

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart neighbor-capability restart-time <i>number</i>
Tree	restart-time
Configurable	False
Platforms	Supported on all platforms

number-of-restarts *number*

Description	The number of times the peer has restarted
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart number-of-restarts <i>number</i>
Tree	number-of-restarts
Configurable	False
Platforms	Supported on all platforms

stale-routes-time *number*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) graceful-restart stale-routes-time <i>number</i>
Tree	stale-routes-time
Range	1 to 3600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

import-policy *reference*

Description	Apply an import policy to received BGP routes
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) import-policy <i>reference</i>
Tree	import-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True

Platforms Supported on all platforms

ipv4-unicast

Description Options related to the IPv4-unicast address family

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [ipv4-unicast](#)

Tree [ipv4-unicast](#)

Configurable True

Platforms Supported on all platforms

active-routes *number*

Description The number of IPv4 unicast received from the peer that are currently used for forwarding

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [ipv4-unicast](#) [active-routes](#) *number*

Tree [active-routes](#)

Configurable False

Platforms Supported on all platforms

admin-state *keyword*

Description Administratively enable or disable the IPv4 unicast address family on the BGP session

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [ipv4-unicast](#) [admin-state](#) *keyword*

Tree [admin-state](#)

Options

- enable
- disable

Configurable True

Platforms Supported on all platforms

advertise-ipv6-next-hops *boolean*

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).

Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast advertise-ipv6-next-hops boolean
Tree	advertise-ipv6-next-hops
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Enter the oper-state context
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast oper-state keyword
Tree	oper-state
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
Platforms	Supported on all platforms

prefix-limit

Description	Options for configuring the maximum number of IPv4 routes allowed to be received from the peer
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast prefix-limit
Tree	prefix-limit
Configurable	True
Platforms	Supported on all platforms

max-received-routes *number*

Description	Maximum number of IPv4 routes that will be accepted from the neighbor, counting routes accepted and rejected by import policies
--------------------	---

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

warning-threshold-pct *number*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Range	0 to 100
Configurable	True
Platforms	Supported on all platforms

receive-ipv6-next-hops *boolean*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast receive-ipv6-next-hops <i>boolean</i>
Tree	receive-ipv6-next-hops
Configurable	True
Platforms	Supported on all platforms

received-routes *number*

Description	The number of IPv4 unicast routes received from the peer, including routes rejected by import policy
--------------------	--

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast received-routes <i>number</i>
Tree	received-routes
Configurable	False
Platforms	Supported on all platforms

rejected-routes *number*

Description	The number of IPv4 unicast routes received from the peer that were rejected by import policy
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast rejected-routes <i>number</i>
Tree	rejected-routes
Configurable	False
Platforms	Supported on all platforms

sent-routes *number*

Description	The number of IPv4 unicast routes advertised as reachable to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv4-unicast sent-routes <i>number</i>
Tree	sent-routes
Configurable	False
Platforms	Supported on all platforms

ipv6-unicast

Description	Options related to the IPv6-unicast address family
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) ipv6-unicast
Tree	ipv6-unicast
Configurable	True
Platforms	Supported on all platforms

active-routes *number*

Description	The number of IPv6 unicast received from the peer that are currently used for forwarding
--------------------	--

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) ipv6-unicast active-routes <i>number</i>
Tree	active-routes
Configurable	False
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the IPv6 unicast address family on the BGP session
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Enter the oper-state context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) ipv6-unicast oper-state <i>keyword</i>
Tree	oper-state
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
Platforms	Supported on all platforms

prefix-limit

Description	Options for configuring the maximum number of IPv6 routes allowed to be received from the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) ipv6-unicast prefix-limit
Tree	prefix-limit

Configurable	True
Platforms	Supported on all platforms

max-received-routes *number*

Description	Maximum number of IPv6 routes that will be accepted from the neighbor, counting routes accepted and rejected by import policies
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) ipv6-unicast prefix-limit max-received-routes <i>number</i>
Tree	max-received-routes
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

warning-threshold-pct *number*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) ipv6-unicast prefix-limit warning-threshold-pct <i>number</i>
Tree	warning-threshold-pct
Range	0 to 100
Configurable	True
Platforms	Supported on all platforms

received-routes *number*

Description	The number of IPv6 unicast routes received from the peer, including routes rejected by import policy
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) ipv6-unicast received-routes <i>number</i>
Tree	received-routes
Configurable	False
Platforms	Supported on all platforms

rejected-routes *number*

Description	The number of IPv6 unicast routes received from the peer that were rejected by import policy
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) ipv6-unicast rejected-routes number
Tree	rejected-routes
Configurable	False
Platforms	Supported on all platforms

sent-routes *number*

Description	The number of IPv6 unicast routes advertised as reachable to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) ipv6-unicast sent-routes number
Tree	sent-routes
Configurable	False
Platforms	Supported on all platforms

last-established *string*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) last-established string
Tree	last-established
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-event *keyword*

Description	Enter the last-event context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) last-event keyword
Tree	last-event
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

Platforms

Supported on all platforms

last-state *keyword***Description**

Previous state of the session

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) last-state <i>keyword</i>
Tree	last-state
Options	<ul style="list-style-type: none"> • idle • connect • active • opensent • openconfirm • established
Configurable	False
Platforms	Supported on all platforms

local-as [as-number](#) *number*

Description	Options related to the local autonomous-system number advertised by this router to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) local-as as-number <i>number</i>
Tree	local-as
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

as-number *number*

Description	<p>The local autonomous system number used to override the global ASN on this session</p> <p>Sets the ASN value that this router sends in its OPEN message towards its peer.</p>
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) local-as as-number <i>number</i>
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

prepend-global-as *boolean*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) local-as as-number <i>number</i> prepend-global-as <i>boolean</i>
Tree	prepend-global-as
Configurable	True
Platforms	Supported on all platforms

prepend-local-as *boolean*

Description	When set to true, the local AS value is prepended to the AS path of inbound routes from the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) local-as as-number <i>number</i> prepend-local-as <i>boolean</i>
Tree	prepend-local-as
Configurable	True
Platforms	Supported on all platforms

local-preference *number*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) local-preference <i>number</i>
Tree	local-preference
Configurable	True
Platforms	Supported on all platforms

maintenance-group *string*

Description	State field to display the maintenance group to which this neighbor belongs to.
--------------------	---

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) maintenance-group <i>string</i>
Tree	maintenance-group
Configurable	False
Platforms	Supported on all platforms

multihop

Description	Configuration parameters specifying the multihop behaviour for an EBGP peer. This is not applicable to an IBGP peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) multihop
Tree	multihop
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	When enabled, the peer is allowed to be indirectly connected by up to N hops, where N is controlled by the maximum-hops parameter. When disabled, multihop is allowed only if the peer type is IBGP. This overrides the group setting for admin-state.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) multihop admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

maximum-hops *number*

Description	This sets the maximum number of routing hops towards the peer. It determines the IP TTL value in originated BGP TCP/IP packets. By default the TTL is set to 1 towards an EBGP peer and 64 towards an IBGP peer. This overrides the group setting for maximum-hops.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) multihop maximum-hops <i>number</i>
Tree	maximum-hops

Range	1 to 255
Configurable	True
Platforms	Supported on all platforms

next-hop-self *boolean*

Description	When set to true, the next-hop in all IPv4-unicast, IPv6-unicast and EVPN BGP routes advertised to the peer, if IBGP, is set equal to the local-address used on this 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-client, IBGP-non-client or redistributed direct/static/aggregate route). When set to false, normal BGP rules from RFC 4271 apply.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) next-hop-self <i>boolean</i>
Tree	next-hop-self
Configurable	True
Platforms	Supported on all platforms

peer-as *number*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) peer-as <i>number</i>
Tree	peer-as
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

peer-group *reference*

Description	A reference to the peer-group template to use for this BGP session This is not immutable.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) peer-group <i>reference</i>
Tree	peer-group
Reference	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>

Configurable	True
Platforms	Supported on all platforms

peer-router-id *string*

Description	The BGP identifier advertised by the peer in its OPEN message
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) peer-router-id <i>string</i>
Tree	peer-router-id
Configurable	False
Platforms	Supported on all platforms

peer-type *keyword*

Description	Enter the peer-type context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) peer-type <i>keyword</i>
Tree	peer-type
Options	<ul style="list-style-type: none"> • <code>ibgp</code> Indicates that the peer is IBGP (<code>local-as == peer-as</code>). • <code>ebgp</code> Indicates that the peer is EBGP (<code>local-as != peer-as</code>).
Configurable	False
Platforms	Supported on all platforms

received-afi-safi *keyword*

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
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) received-afi-safi <i>keyword</i>
Tree	received-afi-safi
Options	<ul style="list-style-type: none"> • <code>ipv4-unicast</code> • <code>ipv6-unicast</code>
Configurable	False
Platforms	Supported on all platforms

received-capabilities *keyword*

Description	List of BGP capabilities received by the local routing device from the peer
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-capabilities <i>keyword</i>
Tree	received-capabilities
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
Platforms	Supported on all platforms

received-end-of-rib *keyword*

Description	List of address families for which the peer has signaled the End of RIB marker
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-end-of-rib <i>keyword</i>
Tree	received-end-of-rib
Options	<ul style="list-style-type: none"> • ipv4-unicast • ipv6-unicast
Configurable	False
Platforms	Supported on all platforms

received-messages

Description	Container for state information about BGP messages received from the peer.
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-messages
Tree	received-messages
Configurable	False

Platforms Supported on all platforms

last-notification-error-code *keyword*

Description The error code in the last NOTIFICATION received from this peer.

Context [network-instance name](#) *string* [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) (*ipv4-address | ipv6-address-with-zone*) [received-messages](#) [last-notification-error-code](#) *keyword*

Tree [last-notification-error-code](#)

Options

- Message Header Error
- Open Message Error
- Update Message Error
- Hold Timer Error
- Finite State Machine Error
- Cease

Configurable False

Platforms Supported on all platforms

last-notification-error-subcode *keyword*

Description The error subcode in the last NOTIFICATION received from the peer.

Context [network-instance name](#) *string* [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) (*ipv4-address | ipv6-address-with-zone*) [received-messages](#) [last-notification-error-subcode](#) *keyword*

Tree [last-notification-error-subcode](#)

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
Platforms	Supported on all platforms

last-notification-time *string*

Description	Timestamp representing the time of the last Notification message received from the peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) received-messages last-notification-time <i>string</i>
Tree	last-notification-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-update-time *string*

Description	The timestamp when the last UPDATE was received from this peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) received-messages last-update-time <i>string</i>
Tree	last-update-time
String Length	20 to 32
Configurable	False

Platforms Supported on all platforms

malformed-updates *number*

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)

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [received-messages](#) [malformed-updates](#) [number](#)

Tree [malformed-updates](#)

Default 0

Configurable False

Platforms Supported on all platforms

queue-depth *number*

Description The number of messages received from the peer currently queued.

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [received-messages](#) [queue-depth](#) [number](#)

Tree [queue-depth](#)

Configurable False

Platforms Supported on all platforms

route-refresh *number*

Description Number of BGP ROUTE_REFRESH messages received from the peer over the lifetime of its configuration or since the last clear.

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [received-messages](#) [route-refresh](#) [number](#)

Tree [route-refresh](#)

Default 0

Configurable False

Platforms Supported on all platforms

total-messages *number*

Description Total number of BGP messages received from the peer over the lifetime of its configuration or since the last clear.

Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-messages total-messages number
Tree	total-messages
Default	0
Configurable	False
Platforms	Supported on all platforms

total-non-updates *number*

Description	Number of BGP NON UPDATE messages received from the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-messages total-non-updates number
Tree	total-non-updates
Configurable	False
Platforms	Supported on all platforms

total-notifications *number*

Description	Number of BGP Notification messages received from the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-messages total-notifications number
Tree	total-notifications
Configurable	False
Platforms	Supported on all platforms

total-updates *number*

Description	Number of BGP UPDATE messages received from the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) received-messages total-updates number
Tree	total-updates
Default	0
Configurable	False

Platforms Supported on all platforms

route-reflector

Description Container with route reflection configuration options.

Context [network-instance name string protocols bgp neighbor peer-address \(ipv4-address | ipv6-address-with-zone\) route-reflector](#)

Tree [route-reflector](#)

Configurable True

Platforms Supported on all platforms

client *boolean*

Description When this is set to true this BGP session is considered an RR client.

Context [network-instance name string protocols bgp neighbor peer-address \(ipv4-address | ipv6-address-with-zone\) route-reflector client boolean](#)

Tree [client](#)

Configurable True

Platforms Supported on all platforms

cluster-id *string*

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.

Context [network-instance name string protocols bgp neighbor peer-address \(ipv4-address | ipv6-address-with-zone\) route-reflector cluster-id string](#)

Tree [cluster-id](#)

Configurable True

Platforms Supported on all platforms

send-community

Description Options for controlling the sending of BGP communities to the peer

Context [network-instance name string protocols bgp neighbor peer-address \(ipv4-address | ipv6-address-with-zone\) send-community](#)

Tree [send-community](#)

Configurable True

Platforms Supported on all platforms

large *boolean*

Description The false setting causes BGP to strip all large (12 byte) BGP communities from all outbound routes advertised to the peer

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [send-community](#) [large](#) [boolean](#)

Tree [large](#)

Configurable True

Platforms Supported on all platforms

standard *boolean*

Description The false setting causes BGP to strip all standard (4 byte) communities from all outbound routes advertised to the peer

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [send-community](#) [standard](#) [boolean](#)

Tree [standard](#)

Configurable True

Platforms Supported on all platforms

send-default-route

Description Options for controlling the generation of default routes towards the peer

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [send-default-route](#)

Tree [send-default-route](#)

Configurable True

Platforms Supported on all platforms

export-policy *reference*

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.

Context [network-instance name](#) [string](#) [protocols](#) [bgp](#) [neighbor](#) [peer-address](#) ([ipv4-address](#) | [ipv6-address-with-zone](#)) [send-default-route](#) [export-policy](#) [reference](#)

Tree [export-policy](#)

Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

ipv4-unicast *boolean*

Description	Enables the sending of a synthetically generated default IPv4 route [0/0] to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) send-default-route ipv4-unicast <i>boolean</i>
Tree	ipv4-unicast
Configurable	True
Platforms	Supported on all platforms

ipv6-unicast *boolean*

Description	Enables the sending of a synthetically generated default IPv6 route [::/0] to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) send-default-route ipv6-unicast <i>boolean</i>
Tree	ipv6-unicast
Configurable	True
Platforms	Supported on all platforms

sent-end-of-rib *keyword*

Description	List of address families for which this router sent the peer an End of RIB marker
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) sent-end-of-rib <i>keyword</i>
Tree	sent-end-of-rib
Options	<ul style="list-style-type: none"> • ipv4-unicast • ipv6-unicast
Configurable	False
Platforms	Supported on all platforms

sent-messages

Description	Container for state information about BGP messages sent to the peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages
Tree	sent-messages
Configurable	False
Platforms	Supported on all platforms

last-notification-error-code *keyword*

Description	The error code in the last NOTIFICATION sent to this peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages last-notification-error-code keyword
Tree	last-notification-error-code
Options	<ul style="list-style-type: none"> • Message Header Error • Open Message Error • Update Message Error • Hold Timer Error • Finite State Machine Error • Cease
Configurable	False
Platforms	Supported on all platforms

last-notification-error-subcode *keyword*

Description	The error subcode in the last NOTIFICATION sent to this peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages last-notification-error-subcode keyword
Tree	last-notification-error-subcode
Options	<ul style="list-style-type: none"> • 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
Platforms	Supported on all platforms

last-notification-time *string*

Description	Timestamp representing the time of the last Notification message sent to the peer.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages last-notification-time <i>string</i>
Tree	last-notification-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

queue-depth *number*

Description	The number of messages queued to be sent to the peer.
--------------------	---

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages queue-depth <i>number</i>
Tree	queue-depth
Configurable	False
Platforms	Supported on all platforms

route-refresh *number*

Description	Number of BGP ROUTE_REFRESH messages sent to the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages route-refresh <i>number</i>
Tree	route-refresh
Default	0
Configurable	False
Platforms	Supported on all platforms

total-messages *number*

Description	Total number of BGP messages sent to the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages total-messages <i>number</i>
Tree	total-messages
Default	0
Configurable	False
Platforms	Supported on all platforms

total-non-updates *number*

Description	Number of BGP NON UPDATE messages sent to the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) sent-messages total-non-updates <i>number</i>
Tree	total-non-updates
Configurable	False
Platforms	Supported on all platforms

total-notifications *number*

Description	Number of BGP Notification messages sent to the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) sent-messages total-notifications <i>number</i>
Tree	total-notifications
Configurable	False
Platforms	Supported on all platforms

total-updates *number*

Description	Number of BGP UPDATE messages sent to the peer over the lifetime of its configuration or since the last clear.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) sent-messages total-updates <i>number</i>
Tree	total-updates
Default	0
Configurable	False
Platforms	Supported on all platforms

session-state *keyword*

Description	Current state of the session
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) session-state <i>keyword</i>
Tree	session-state
Options	<ul style="list-style-type: none"> • idle • connect • active • opensent • openconfirm • established
Configurable	False
Platforms	Supported on all platforms

slow-peer *keyword*

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.
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) slow-peer keyword
Tree	slow-peer
Options	<ul style="list-style-type: none"> • yes • no • unknown
Configurable	False
Platforms	Supported on all platforms

timers

Description	Enter the timers context
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) timers
Tree	timers
Configurable	True
Platforms	Supported on all platforms

connect-retry *number*

Description	The time interval in seconds between successive attempts to establish a session with a peer
Context	network-instance name string protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) timers connect-retry number
Tree	connect-retry
Range	1 to 65535
Units	seconds
Configurable	True
Platforms	Supported on all platforms

hold-time *number*

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.

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) timers hold-time <i>number</i>
Tree	hold-time
Range	0 3 to 65535
Units	seconds
Configurable	True
Platforms	Supported on all platforms

keepalive-interval *number*

Description	<p>The interval in seconds between successive keepalive messages sent to the peer</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) timers keepalive-interval <i>number</i>
Tree	keepalive-interval
Range	0 to 21845
Units	seconds
Configurable	True
Platforms	Supported on all platforms

minimum-advertisement-interval *number*

Description	<p>The value assigned to the MinRouteAdvertisementIntervalTimer of RFC 4271, for both EBGp and IBGP sessions</p> <p>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.</p>
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) timers minimum-advertisement-interval <i>number</i>
Tree	minimum-advertisement-interval
Range	1 to 255
Units	seconds

Configurable	True
Platforms	Supported on all platforms

negotiated-hold-time *number*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) timers negotiated-hold-time <i>number</i>
Tree	negotiated-hold-time
Configurable	False
Platforms	Supported on all platforms

negotiated-keepalive-interval *number*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) timers negotiated-keepalive-interval <i>number</i>
Tree	negotiated-keepalive-interval
Configurable	False
Platforms	Supported on all platforms

next-connect-retry-time *string*

Description	The time when the next connect retry attempt will occur
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (ipv4-address ipv6-address-with-zone) timers next-connect-retry-time <i>string</i>
Tree	next-connect-retry-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Debug traceoptions for BGP
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

flag name keyword

Description	Tracing parameters
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) trace-options flag name keyword
Tree	flag
Configurable	True
Platforms	Supported on all platforms

name keyword

Description	Enter the name context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) trace-options flag name keyword
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
Platforms	Supported on all platforms

modifier *keyword*

Description	Enter the modifier context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) trace-options flag name <i>keyword</i> modifier <i>keyword</i>
Tree	modifier
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
Platforms	Supported on all platforms

transport

Description	Enter the transport context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>) transport
Tree	transport
Configurable	True
Platforms	Supported on all platforms

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

Description	<p>The local TCP endpoint of used for the BGP session</p> <p>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.</p>
--------------------	--

This address must be the primary address of an interface, otherwise the session will not come up.

Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) transport local-address (<i>ipv4-address ipv6-address string</i>)
Tree	local-address
Configurable	True
Platforms	Supported on all platforms

local-port *number*

Description	Local TCP port used for the TCP connection to the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) transport local-port <i>number</i>
Tree	local-port
Configurable	False
Platforms	Supported on all platforms

passive-mode *boolean*

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) transport passive-mode <i>boolean</i>
Tree	passive-mode
Configurable	True
Platforms	Supported on all platforms

remote-port *number*

Description	Remote TCP port used by the peer for its TCP connection to the local router
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) transport remote-port <i>number</i>
Tree	remote-port
Configurable	False
Platforms	Supported on all platforms

tcp-mss number

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) transport tcp-mss number
Tree	tcp-mss
Range	536 to 9446
Units	bytes
Configurable	True
Platforms	Supported on all platforms

under-maintenance boolean

Description	State field to determine if this bgp neighbor is in maintenance mode.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) under-maintenance boolean
Tree	under-maintenance
Configurable	False
Platforms	Supported on all platforms

oper-state keyword

Description	Enter the oper-state context
Context	network-instance name <i>string</i> protocols bgp oper-state keyword
Tree	oper-state
Options	<ul style="list-style-type: none"> • up Operational state of BGP is up. • down Operational state of BGP is down.
Configurable	False
Platforms	Supported on all platforms

preference

Description	Options for controlling the route table preference of BGP routes
--------------------	--

Context	network-instance name <i>string</i> protocols bgp preference
Tree	preference
Configurable	True
Platforms	Supported on all platforms

ebgp number

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.
Context	network-instance name <i>string</i> protocols bgp preference ebgp number
Tree	ebgp
Default	170
Configurable	True
Platforms	Supported on all platforms

ibgp number

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.
Context	network-instance name <i>string</i> protocols bgp preference ibgp number
Tree	ibgp
Default	170
Configurable	True
Platforms	Supported on all platforms

route-advertisement

Description	Options for controlling route advertisement behavior
Context	network-instance name <i>string</i> protocols bgp route-advertisement
Tree	route-advertisement
Configurable	True
Platforms	Supported on all platforms

rapid-withdrawal *boolean*

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.
Context	network-instance name <i>string</i> protocols bgp route-advertisement rapid-withdrawal <i>boolean</i>
Tree	rapid-withdrawal
Default	false
Configurable	True
Platforms	Supported on all platforms

wait-for-fib-install *boolean*

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.
Context	network-instance name <i>string</i> protocols bgp route-advertisement wait-for-fib-install <i>boolean</i>
Tree	wait-for-fib-install
Default	true
Configurable	True
Platforms	Supported on all platforms

route-reflector

Description	Container with route reflection configuration options.
Context	network-instance name <i>string</i> protocols bgp route-reflector
Tree	route-reflector
Configurable	True
Platforms	Supported on all platforms

client *boolean*

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.
--------------------	--

Context	network-instance name <i>string</i> protocols bgp route-reflector client <i>boolean</i>
Tree	client
Default	false
Configurable	True
Platforms	Supported on all platforms

cluster-id *string*

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.
Context	network-instance name <i>string</i> protocols bgp route-reflector cluster-id <i>string</i>
Tree	cluster-id
Configurable	True
Platforms	Supported on all platforms

router-id (*ipv4-address* | *ipv6-address*)

Description	The BGP identifier used by this BGP instance in all of its OPEN messages Any non-zero value is supported.
Context	network-instance name <i>string</i> protocols bgp router-id (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	router-id
Configurable	True
Platforms	Supported on all platforms

send-community

Description	Options for controlling the sending of BGP communities to all peers
Context	network-instance name <i>string</i> protocols bgp send-community
Tree	send-community
Configurable	True
Platforms	Supported on all platforms

large *boolean*

Description	The false setting causes BGP to strip all large (12 byte) BGP communities from all outbound routes advertised to peers
--------------------	--

Context	network-instance name <i>string</i> protocols bgp send-community large <i>boolean</i>
Tree	large
Default	true
Configurable	True
Platforms	Supported on all platforms

standard *boolean*

Description	The false setting causes BGP to strip all standard (4 byte) communities from all outbound routes advertised to peers
Context	network-instance name <i>string</i> protocols bgp send-community standard <i>boolean</i>
Tree	standard
Default	true
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Container for BGP statistics.
Context	network-instance name <i>string</i> protocols bgp statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

disabled-peers *number*

Description	The number of configured BGP peers that are administratively disabled
Context	network-instance name <i>string</i> protocols bgp statistics disabled-peers <i>number</i>
Tree	disabled-peers
Configurable	False
Platforms	Supported on all platforms

dynamic-peers *number*

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
--------------------	---

Context	network-instance name <i>string</i> protocols bgp statistics dynamic-peers <i>number</i>
Tree	dynamic-peers
Configurable	False
Platforms	Supported on all platforms

path-memory *number*

Description	The total number of bytes required to store the path attribute objects used by all received BGP routes
Context	network-instance name <i>string</i> protocols bgp statistics path-memory <i>number</i>
Tree	path-memory
Default	0
Configurable	False
Platforms	Supported on all platforms

total-active-routes *number*

Description	The total number of received BGP routes that are active (installed for forwarding), summed across all address families
Context	network-instance name <i>string</i> protocols bgp statistics total-active-routes <i>number</i>
Tree	total-active-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

total-paths *number*

Description	The total number of path attribute objects used by all received BGP routes
Context	network-instance name <i>string</i> protocols bgp statistics total-paths <i>number</i>
Tree	total-paths
Default	0
Configurable	False
Platforms	Supported on all platforms

total-peers *number*

Description	The total number of configured BGP peers
Context	network-instance name <i>string</i> protocols bgp statistics total-peers <i>number</i>
Tree	total-peers
Configurable	False
Platforms	Supported on all platforms

total-prefixes *number*

Description	The total number of unique NLRI contained in all received BGP routes associated with the BGP instance or the peer-group.
Context	network-instance name <i>string</i> protocols bgp statistics total-prefixes <i>number</i>
Tree	total-prefixes
Configurable	False
Platforms	Supported on all platforms

total-received-routes *number*

Description	The total number of received BGP routes, summed across all address families
Context	network-instance name <i>string</i> protocols bgp statistics total-received-routes <i>number</i>
Tree	total-received-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

up-peers *number*

Description	The number of configured BGP peers that are currently in the established state
Context	network-instance name <i>string</i> protocols bgp statistics up-peers <i>number</i>
Tree	up-peers
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Debug traceoptions for BGP
Context	network-instance name <i>string</i> protocols bgp trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

flag *name keyword*

Description	Tracing parameters
Context	network-instance name <i>string</i> protocols bgp trace-options flag name <i>keyword</i>
Tree	flag
Configurable	True
Platforms	Supported on all platforms

name *keyword*

Description	Enter the name context
Context	network-instance name <i>string</i> protocols bgp trace-options flag name <i>keyword</i>
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
Platforms	Supported on all platforms

modifier *keyword*

Description	Enter the modifier context
Context	network-instance name <i>string</i> protocols bgp trace-options flag name <i>keyword</i> modifier keyword
Tree	modifier
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
Platforms	Supported on all platforms

transport

Description	Options related to the TCP transport of BGP sessions
Context	network-instance name <i>string</i> protocols bgp transport
Tree	transport
Configurable	True
Platforms	Supported on all platforms

single-hop-connected-check *boolean*

Description	<p>Control whether a single-hop BGP session should be allowed to setup if its 'related interface' is down.</p> <p>If single-hop-connected-check is false, a single-hop BGP session (EBGP or IBGP) to any IPv4 or IPv6 neighbor address is permitted to establish if there is ANY valid (IPv6 global unicast, IPv4 link-local, or IPv4 global) route to that neighbor address, regardless of whether the 'related interface' is up or down.</p> <p>If single-hop-connected-check is true (default value), a single-hop BGP session (EBGP or IBGP) to any IPv4 or IPv6 neighbor address is only</p>
--------------------	---

permitted to transition from idle to a higher state if the 'related interface' is up.

The 'related interface' of a single hop peer is the subinterface associated with the IPv6 link local neighbor address or else the subinterface with a primary or secondary IP address and prefix-length that covers the neighbor address.

Context	network-instance name <i>string</i> protocols bgp transport single-hop-connected-check <i>boolean</i>
Tree	single-hop-connected-check
Default	true
Configurable	True
Platforms	Supported on all platforms

tcp-mss *number*

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
Context	network-instance name <i>string</i> protocols bgp transport tcp-mss <i>number</i>
Tree	tcp-mss
Range	536 to 9446
Default	1024
Configurable	True
Platforms	Supported on all platforms

under-maintenance *boolean*

Description	State field to determine if the bgp instance is in maintenance mode.
Context	network-instance name <i>string</i> protocols bgp under-maintenance <i>boolean</i>
Tree	under-maintenance
Configurable	False
Platforms	Supported on all platforms

bgp-evpn

Description	Enable the bgp-evpn context
Context	network-instance name <i>string</i> protocols bgp-evpn
Tree	bgp-evpn

Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bgp-instance *id reference*

Description	The bgp-evpn instances configured in net-instance
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id reference
Tree	bgp-instance
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	1

id *reference*

Description	Enter the id context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id reference
Reference	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id number
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

admin-state *keyword*

Description	Configurable state of the bgp evpn instance.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id reference admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

default-admin-tag *number*

Description	The admin-tag that can be used by an export policy to match all the bgp-evpn routes for the bgp-instance.
--------------------	---

Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> default-admin-tag <i>number</i>
Tree	default-admin-tag
Range	0 to 4294967295
Default	0
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ecmp *number*

Description	The supported range of ECMP values for layer-2 aliasing (in mac-vrf instances) or layer-3 ecmp (in routed instances).
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> ecmp <i>number</i>
Tree	ecmp
Range	1 to 8
Default	1
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

encapsulation-type *keyword*

Description	Encapsulation type of the bgp-evpn instance.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> encapsulation-type <i>keyword</i>
Tree	encapsulation-type
Default	vxlan
Options	<ul style="list-style-type: none"> • vxlan • mpls
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

evi *number*

Description	EVPN Instance identifier associated to the bgp-evpn instance. Used for auto-derivation of:
--------------------	---

In addition, the `evi` value is used for the EVPN Multi-Homing Designated Forwarder (DF) Election.

Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> evi number
Tree	evi
Range	1 to 65535
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ingress-replication-bum-label *boolean*

Description	Use the same label as the one advertised for unicast traffic.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> ingress-replication-bum-label <i>boolean</i>
Tree	ingress-replication-bum-label
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-down-reason *keyword*

Description	The reason for the bgp-instance being down
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • admin-disabled • no-nexthop-address • no-evi • network-instance-oper-down • no-vxlan-interface • ethernet-segment-multiple-subinterfaces • vxlan_interface_no_source_ip_address • bgp-vpn-instance-oper-down • no-mpls-label
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-state *keyword*

Description	This leaf contains the operational state of bgp-instance.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that

the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

routes

Description	Enter the routes context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes
Tree	routes
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bridge-table

Description	Enable the bridge-table context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table
Tree	bridge-table
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

inclusive-mcast

Description	Enter the inclusive-mcast context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table inclusive-mcast
Tree	inclusive-mcast
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

advertise *boolean*

Description	If set to true an inclusive multicast route will be advertised in this evpn instance.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table inclusive-mcast advertise <i>boolean</i>

Tree	advertise
Default	true
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

originating-ip (*ipv4-address* | *ipv6-address*)

Description	The originating ip-address that the inclusive multicast route will be advertised with in this evpn instance
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table inclusive-mcast originating-ip (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	originating-ip
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-ip

Description	Enter the mac-ip context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table mac-ip
Tree	mac-ip
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

advertise *boolean*

Description	If set to true then local mac's and local mac-ip pairs will be advertised in this evpn instance
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table mac-ip advertise <i>boolean</i>
Tree	advertise
Default	true
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

advertise-arp-nd-only-with-mac-table-entry *boolean*

Description	If set to true then local mac-ip records will be advertised in this evpn instance only when we have a local mac in the mac-table
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table mac-ip advertise-arp-nd-only-with-mac-table-entry <i>boolean</i>
Tree	advertise-arp-nd-only-with-mac-table-entry
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

next-hop (*keyword* | *ipv4-address* | *ipv6-address*)

Description	The ip-address that will be used as the bgp next-hop for all routes advertised in this evpn instance.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table next-hop (<i>keyword</i> <i>ipv4-address</i> <i>ipv6-address</i>)
Tree	next-hop
Default	use-system-ipv4-address
Options	<ul style="list-style-type: none"> • use-system-ipv4-address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vlan-aware-bundle-eth-tag *number*

Description	<p>Configures the Ethernet Tag ID to be encoded in the EVPN routes for control-plane interoperability mode with VLAN-aware bundle services.</p> <p>When set to a non-zero value, all the EVPN routes advertised for the MAC-VRF will be advertised with this value into the ethernet-tag-id field of the routes.</p> <p>On reception of EVPN routes with non-zero ethernet-tag-id, BGP will import the routes based on the import route-target as usual. However, the system checks the received ethernet-tag-id field and will process only those routes whose ethernet-tag-id match the local vlan-aware-bundle-eth-tag value.</p>
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes bridge-table vlan-aware-bundle-eth-tag <i>number</i>
Tree	vlan-aware-bundle-eth-tag
Range	0 to 16777215
Default	0

Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

route-table

Description	Enable the route-table context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes route-table
Tree	route-table
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-ip

Description	Enter the mac-ip context
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes route-table mac-ip
Tree	mac-ip
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

advertise-gateway-mac *boolean*

Description	If set to true in an ip-vrf where bgp-evpn is enabled, a MAC/IP route containing the gateway-MAC is advertised. This gateway-MAC matches the MAC advertised along with the EVPN IFL routes type 5 for the ip-vrf network-instance. This advertisement is needed so that the EVPN IFL (Interface-Less) model in the ip-vrf can interoperate with a remote system working in EVPN IFF (Interface-ful) Unnumbered mode.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> routes route-table mac-ip advertise-gateway-mac <i>boolean</i>
Tree	advertise-gateway-mac
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vxlan-interface *reference*

Description	Identifier of vxlan-interface used in this bgp-instance.
Context	network-instance name <i>string</i> protocols bgp-evpn bgp-instance id <i>reference</i> vxlan-interface <i>reference</i>
Tree	vxlan-interface
Reference	network-instance name <i>string</i> vxlan-interface name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bgp-vpn

Description	Enable the bgp-vpn context
Context	network-instance name <i>string</i> protocols bgp-vpn
Tree	bgp-vpn
Configurable	True
Platforms	Supported on all platforms

bgp-instance [id](#) *number*

Description	List of bgp-vpn instances configured in the network-instance. Only one instance allowed in the current release.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i>
Tree	bgp-instance
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

id *number*

Description	The index of the bgp-vpn instance
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i>
Range	1 to 2
Configurable	True
Platforms	Supported on all platforms

export-policy *reference*

Description	Apply an export policy to advertised BGP routes
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> export-policy reference
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

import-policy *reference*

Description	Apply an import policy to received BGP routes
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> import-policy reference
Tree	import-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	Reason for bgp-instance being down
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> oper-down-reason keyword
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • no-loopback-address-or-rd • no-autonomous-system-or-rt • network-instance-oper-down • none
Configurable	False
Platforms	Supported on all platforms

route-distinguisher

Description	Route Distinguisher (RD) of the bgp-vpn instance.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-distinguisher

Tree	route-distinguisher
Configurable	True
Platforms	Supported on all platforms

rd (*string* | *string* | *string* | *string*)

Description	Route Distinguisher (RD) configured in the bgp-vpn instance. When used for evpn and if not configured, the RD is auto-derived with the format <ip-address>:<evi> where 'ip-address' is the ipv4 address associated to the subinterface lo0.1.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-distinguisher rd (<i>string</i> <i>string</i> <i>string</i> <i>string</i>)
Tree	rd
Configurable	True
Platforms	Supported on all platforms

route-distinguisher-origin *keyword*

Description	Origin of the operational Route Distinguisher (RD) of the bgp-vpn instance. 'Auto-derived-from-evi' refers to an RD that is automatically allocated with the format <ip-address>:<evi> where 'ip-address' is the ipv4 address associated to the subinterface lo0.1. 'Manual' refers to an RD that is configured. 'None' indicates that the RD is neither configured nor auto-derived.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-distinguisher route-distinguisher-origin <i>keyword</i>
Tree	route-distinguisher-origin
Options	<ul style="list-style-type: none"> • auto-derived-from-evi • auto-derived-from-system-ip:0 • manual • none
Configurable	False
Platforms	Supported on all platforms

route-target

Description	Route Target (RT) of the bgp-vpn instance.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-target
Tree	route-target

Configurable	True
Platforms	Supported on all platforms

export-route-target-origin *keyword*

Description	Origin of the operational export Route Target (RT) of the bgp-vpn instance. 'Auto-derived-from-evi' refers to an RT that is automatically allocated with the format <asn>:<evi> where 'asn' is the autonomous-system-number configured in the network-instance default. 'Manual' refers to an export RT that is configured. 'None' indicates that the export RT is neither configured nor auto-derived.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-target export-route-target-origin <i>keyword</i>
Tree	export-route-target-origin
Options	<ul style="list-style-type: none"> • auto-derived-from-evi • manual • none
Configurable	False
Platforms	Supported on all platforms

export-rt (*string* | *string* | *string*)

Description	Export Route Target (RT) in the bgp-vpn instance. When used for evpn and if not configured, the RT is auto-derived with the format <asn>:<evi> where 'asn' is the autonomous-system configured in the network-instance default.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-target export-rt (<i>string</i> <i>string</i> <i>string</i> <i>string</i> <i>string</i> <i>string</i> <i>string</i> <i>string</i> <i>string</i> <i>string</i>)
Tree	export-rt
Configurable	True
Platforms	Supported on all platforms

import-route-target-origin *keyword*

Description	Origin of the operational import Route Target (RT) of the bgp-vpn instance. 'Auto-derived-from-evi' refers to an RT that is automatically allocated with the format <asn>:<evi> where 'asn' is the autonomous-system-number configured in the network-instance default. 'Manual' refers to an import RT that is configured. 'None' indicates that the import RT is neither configured nor auto-derived.
--------------------	---

Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-target import-route-target-origin <i>keyword</i>
Tree	import-route-target-origin
Options	<ul style="list-style-type: none"> • auto-derived-from-evi • manual • none
Configurable	False
Platforms	Supported on all platforms

import-rt (*string* | *string* | *string*)

Description	Import Route Target (RT) in the bgp-vpn instance. When used for evpn and if not configured, the RT is auto-derived with the format <asn>:<evi> where 'asn' is the autonomous-system configured in the network-instance default.
Context	network-instance name <i>string</i> protocols bgp-vpn bgp-instance id <i>number</i> route-target import-rt (<i>string</i> <i>string</i>)
Tree	import-rt
Configurable	True
Platforms	Supported on all platforms

gribi

Description	Container for gRIBI configuration and state.
Context	network-instance name <i>string</i> protocols gribi
Tree	gribi
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description	<p>Administratively enable or disable gRIBI support.</p> <p>When this is set to disable all IP entries and next-hop-groups associated with the network-instance are deleted from the gRIBI server database and the recovery of this state depends on the gRIBI clients to re-signal all of the deleted entries. While in a disabled state, no entries are accepted for this network-instance. (This is the same behavior when the network-instance does not exist at all.)</p>
--------------------	--

Context	network-instance name <i>string</i> protocols gribi admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

default-metric *number*

Description	Set the route table metric to use for all gRIBI-created IPv4 and IPv6 routes
Context	network-instance name <i>string</i> protocols gribi default-metric <i>number</i>
Tree	default-metric
Default	1
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

default-preference *number*

Description	Lower values indicate a higher degree of preference when deciding the route to use from different protocols.
Context	network-instance name <i>string</i> protocols gribi default-preference <i>number</i>
Tree	default-preference
Range	0 to 255
Default	4
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

max-ecmp-hash-buckets-per-next-hop-group *number*

Description	<p>Specifies the maximum number of ECMP hash buckets per next-hop-group.</p> <p>An error is returned to any gRIBI client that attempts to program more than this number of next-hops in a single next-hop-group.</p> <p>Weighted ECMP weights are normalized based on this number of hash buckets.</p>
--------------------	--

Context	network-instance name <i>string</i> protocols gribi max-ecmp-hash-buckets-per-next-hop-group <i>number</i>
Tree	max-ecmp-hash-buckets-per-next-hop-group
Range	1 to 128
Default	128
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

maximum-routes *number*

Description	Specifies the maximum number of gRIBI routes (sum of IPv4 and IPv6 entries). A value of 0 signifies no limit.
Context	network-instance name <i>string</i> protocols gribi maximum-routes <i>number</i>
Tree	maximum-routes
Default	0
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

igmp

Description	Enable the igmp context
Context	network-instance name <i>string</i> protocols igmp
Tree	igmp
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description	Administratively enable or disable the IGMP instance.
Context	network-instance name <i>string</i> protocols igmp admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> enable

	<ul style="list-style-type: none"> • disable
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interface [interface-name](#) *reference*

Description	List of IGMP interfaces
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i>
Tree	interface
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interface-name *reference*

Description	Reference to a specific subinterface of the form <interface-name>.<subinterface-index>
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i>
Reference	network-instance name <i>string</i> interface name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description	Administratively enable or disable the IGMP protocol for this interface. Used to administratively enable or disable the IGMP protocol on a routed subinterface
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

counters

Description Global IGMP counters.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [counters](#)

Tree [counters](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

error

Description Error message statistics.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [counters error](#)

Tree [error](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

bad-encoding

Description Badly encoded.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [counters error bad-encoding](#)

Tree [bad-encoding](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

bad-length

Description Bad length.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [counters error bad-length](#)

Tree [bad-length](#)

Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

import-policy-drops

Description	Number of times we matched the host IP address or group or source addresses specified in the import policy.
Context	network-instance name string protocols igmp interface interface-name reference counters error import-policy-drops
Tree	import-policy-drops
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

local-scope

Description	Link-local scope multicast group address.
Context	network-instance name string protocols igmp interface interface-name reference counters error local-scope
Tree	local-scope
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

missing-router-alert

Description	Router alert flag is not set.
Context	network-instance name string protocols igmp interface interface-name reference counters error missing-router-alert
Tree	missing-router-alert
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

non-local

Description	Non-local sender source IP address.
--------------------	-------------------------------------

Context	network-instance name <i>string</i> protocols igmp interface interface-name reference counters error non-local
Tree	non-local
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

out-of-memory-drops

Description	Number of times a join is dropped because we ran out of memory.
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference counters error out-of-memory-drops
Tree	out-of-memory-drops
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

reached-maximum-number-group-sources

Description	Number of times a join is dropped because we reached the maximum number group-source combinations.
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference counters error reached-maximum-number-group-sources
Tree	reached-maximum-number-group-sources
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

reached-maximum-number-groups

Description	Number of times a join is dropped because we reached the maximum number of groups.
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference counters error reached-maximum-number-groups
Tree	reached-maximum-number-groups
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

reached-maximum-number-sources

Description	Number of times a join is dropped because we reached the maximum number of sources per group.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> counters error reached-maximum-number-sources
Tree	reached-maximum-number-sources
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

reserved-scope

Description	Reserved scope multicast group address.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> counters error reserved-scope
Tree	reserved-scope
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

unknown-type

Description	Unknown type.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> counters error unknown-type
Tree	unknown-type
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

wrong-version

Description	Wrong version.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> counters error wrong-version
Tree	wrong-version
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

received

Description	Received message statistics.
Context	network-instance name string protocols igmp interface interface-name reference counters received
Tree	received
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

drops

Description	Total number of dropped packets.
Context	network-instance name string protocols igmp interface interface-name reference counters received drops
Tree	drops
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

general-queries

Description	General Queries.
Context	network-instance name string protocols igmp interface interface-name reference counters received general-queries
Tree	general-queries
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-queries

Description	Group Specific Queries.
Context	network-instance name string protocols igmp interface interface-name reference counters received group-queries
Tree	group-queries
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-source-queries

Description	Group and Source Specific Queries.
Context	network-instance name string protocols igmp interface interface-name reference counters received group-source-queries
Tree	group-source-queries
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

leaves

Description	Leaves context
Context	network-instance name string protocols igmp interface interface-name reference counters received leaves
Tree	leaves
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

v1-reports

Description	V1 Reports.
Context	network-instance name string protocols igmp interface interface-name reference counters received v1-reports
Tree	v1-reports
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

v2-reports

Description	V2 Reports.
Context	network-instance name string protocols igmp interface interface-name reference counters received v2-reports
Tree	v2-reports
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

v3-reports

Description	V3 Reports.
Context	network-instance name string protocols igmp interface interface-name reference counters received v3-reports
Tree	v3-reports
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

transmitted

Description	Transmit message statistics.
Context	network-instance name string protocols igmp interface interface-name reference counters transmitted
Tree	transmitted
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

errors

Description	Transmission Errors.
Context	network-instance name string protocols igmp interface interface-name reference counters transmitted errors
Tree	errors
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

general-queries

Description	General Queries.
Context	network-instance name string protocols igmp interface interface-name reference counters transmitted general-queries
Tree	general-queries
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-queries

Description	Group Specific Queries.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> counters transmitted group-queries
Tree	group-queries
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-source-queries

Description	Group and Source Specific Queries.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> counters transmitted group-source-queries
Tree	group-source-queries
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-count *number*

Description	The number of multicast groups which have been learned this interface.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> group-count <i>number</i>
Tree	group-count
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

import-policy *reference*

Description	Apply an import policy. The length of the policy name should not exceed 32 characters.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> import-policy <i>reference</i>
Tree	import-policy
Reference	routing-policy <i>policy name</i> <i>string</i>
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

max-group-sources *number*

Description MAX number of IGMP group/source combinations for this interface, 0 means no limit

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [max-group-sources](#) *number*

Tree [max-group-sources](#)

Range 0 to 4096

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

max-groups *number*

Description MAX number of IGMP Groups for this interface, 0 means no limit.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [max-groups](#) *number*

Tree [max-groups](#)

Range 0 to 4096

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

max-sources *number*

Description MAX number of IGMP sources per group for this interface, 0 means no limit

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference [max-sources](#) *number*

Tree [max-sources](#)

Range 0 to 512

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

membership-groups

Description	List of IGMP Membership information.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups
Tree	membership-groups
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group [group string](#)

Description	Multicast group membership.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group string
Tree	group
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group *string*

Description	Multicast address.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group string
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

expiry-time *number*

Description	The time left before multicast group timeout.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group string expiry-time number
Tree	expiry-time
Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

filter-mode *keyword*

Description	Enter the filter-mode context
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference membership-groups group group <i>string</i> filter-mode keyword
Tree	filter-mode
Options	<ul style="list-style-type: none"> include In include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter exclude In exclude mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-type *keyword*

Description	Enter the group-type context
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference membership-groups group group <i>string</i> group-type keyword
Tree	group-type
Options	<ul style="list-style-type: none"> static This group entry was statically configured. dynamic This group entry was learned by the protocol. bgp-smet This group entry was learned from a bgp SMET route. bgp-sync This group entry was learned from a bgp JOIN SYNC route.
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

igmp-compatibility-mode *keyword*

Description	Compatibility with older version routers.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> igmp-compatibility-mode <i>keyword</i>
Tree	igmp-compatibility-mode
Options	<ul style="list-style-type: none"> • 1 • 2 • 3
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

last-reporter (*ipv4-address* | *ipv6-address*)

Description	The last host address which has sent the report to join the multicast group.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> last-reporter (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	last-reporter
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source [source](#) *string*

Description	Source addresses of multicast.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> source source <i>string</i>
Tree	source
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source *string*

Description	Source address of multicast.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> source source <i>string</i>

Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

expiry-time *number*

Description	The time left before multicast group timeout.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> source source <i>string</i> expiry-time <i>number</i>
Tree	expiry-time
Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

forwarding-state *keyword*

Description	Traffic forwarding state on this port.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> source source <i>string</i> forwarding-state <i>keyword</i>
Tree	forwarding-state
Options	<ul style="list-style-type: none"> • forward • block
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source-type *keyword*

Description	Enter the source-type context
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> source source <i>string</i> source-type <i>keyword</i>
Tree	source-type
Options	<ul style="list-style-type: none"> • static <p>This group entry was statically configured.</p> • dynamic

This group entry was learned by the protocol.

- bgp-smet

This group entry was learned from a bgp SMET route.

- bgp-sync

This group entry was learned from a bgp JOIN SYNC route.

Configurable

False

Platforms

7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

up-time number

Description

The time elapsed since this entry was created.

Context

[network-instance name](#) *string* [protocols igmp interface interface-name](#) *reference* [membership-groups group group](#) *string* [source source](#) *string* *up-time number*

Tree

[up-time](#)

Units

seconds

Configurable

False

Platforms

7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

up-time number

Description

The time elapsed since this entry was created.

Context

[network-instance name](#) *string* [protocols igmp interface interface-name](#) *reference* [membership-groups group group](#) *string* *up-time number*

Tree

[up-time](#)

Units

seconds

Configurable

False

Platforms

7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

v1-host-timer number

Description

The time remaining until the local router will assume that there are no longer any version 1 members.

Context

[network-instance name](#) *string* [protocols igmp interface interface-name](#) *reference* [membership-groups group group](#) *string* *v1-host-timer number*

Tree

[v1-host-timer](#)

Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

v2-host-timer *number*

Description	The time remaining until the local router will assume that there are no longer any version 2 members.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> membership-groups group group <i>string</i> v2-host-timer <i>number</i>
Tree	v2-host-timer
Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-state *keyword*

Description	The operational state of the IGMP interface. This simply tracks the operational state of the subinterface.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-version *number*

Description	The operational IGMP version on this interface
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> oper-version <i>number</i>
Tree	oper-version
Range	1 to 3
Configurable	False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

querier

Description Enter the querier context

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference querier

Tree [querier](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

address *string*

Description The address of the IGMP Querier on the IP subnet to which this interface is attached.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference querier address string

Tree [address](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

expiry-time *number*

Description The time remaining before this querier is aged out.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#)
reference querier expiry-time number

Tree [expiry-time](#)

Units seconds

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

up-time *number*

Description The time since this querier was last elected.

Context	network-instance name <i>string</i> protocols igmp interface interface-name reference querier up-time <i>number</i>
Tree	up-time
Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

query-interval *number*

Description	Interval at which the router sends the IGMP membership queries
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference query-interval <i>number</i>
Tree	query-interval
Range	2 to 1024
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

query-last-member-interval *number*

Description	Interval at which Group-Specific-Query packets are transmitted
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference query-last-member-interval <i>number</i>
Tree	query-last-member-interval
Range	1 to 1023
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

query-response-interval *number*

Description	Time to wait to receive a response to the IGMP membership query from the host
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference query-response-interval <i>number</i>
Tree	query-response-interval
Range	1 to 1023
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

router-alert-check *boolean*

Description Enable or disable router alert checking for IGMP messages received on this interface.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#) *reference* [router-alert-check](#) *boolean*

Tree [router-alert-check](#)

Default true

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

ssm

Description Container to configure Source specific multicast (SSM) options.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#) *reference* [ssm](#)

Tree [ssm](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

mappings

Description A list of source specific multicast (SSM) mappings.

Context [network-instance name](#) *string* [protocols igmp interface interface-name](#) *reference* [ssm mappings](#)

Tree [mappings](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-range [start](#) *string* [end](#) *string*

Description A Source Specific Multicast (SSM) mapping.
This allows IGMP v2 hosts to be able to join in SSM environments by translating IGMP v2 reports into IGMP v3 reports. The request in an IGMP

	v2 join is sent toward the source address found by matching the multicast address.
Context	network-instance name string protocols igmp interface interface-name reference ssm mappings group-range start string end string
Tree	group-range
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
start string	
Description	Start of the group range.
Context	network-instance name string protocols igmp interface interface-name reference ssm mappings group-range start string end string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
end string	
Description	End of the group range.
Context	network-instance name string protocols igmp interface interface-name reference ssm mappings group-range start string end string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
source source string	
Description	Multicast source address list.
Context	network-instance name string protocols igmp interface interface-name reference ssm mappings group-range start string end string source source string
Tree	source
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
Min. Elements	1

source *string*

Description	Multicast source address.
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference ssm mappings group-range start <i>string</i> end <i>string</i> source source <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

static

Description	Container to configure static <S,G>s for this interface.
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference static
Tree	static
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-range [start *string* end *string*](#)

Description	Enter the group-range list instance
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference static group-range start <i>string</i> end <i>string</i>
Tree	group-range
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

start *string*

Description	Start of the group range.
Context	network-instance name <i>string</i> protocols igmp interface interface-name reference static group-range start <i>string</i> end <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

end string

Description	End of the group range.
Context	network-instance name string protocols igmp interface interface-name reference static group-range start string end string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source source string

Description	Multicast source address list.
Context	network-instance name string protocols igmp interface interface-name reference static group-range start string end string source source string
Tree	source
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source string

Description	Multicast source address.
Context	network-instance name string protocols igmp interface interface-name reference static group-range start string end string source source string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

starg

Description	any source address (*,G)
Context	network-instance name string protocols igmp interface interface-name reference static group-range start string end string starg
Tree	starg
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

subnet-check *boolean*

Description	This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> subnet-check <i>boolean</i>
Tree	subnet-check
Default	true
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

version *number*

Description	IGMP Version
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i> version <i>number</i>
Tree	version
Range	1 to 3
Default	3
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-state *keyword*

Description	Used to report operational state of the IGMP instance.
Context	network-instance name <i>string</i> protocols igmp oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

query-interval *number*

Description	Interval at which the router sends the IGMP membership queries
Context	network-instance name <i>string</i> protocols igmp query-interval <i>number</i>
Tree	query-interval
Range	2 to 1024
Default	125
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

query-last-member-interval *number*

Description	Interval at which Group-Specific-Query packets are transmitted
Context	network-instance name <i>string</i> protocols igmp query-last-member-interval <i>number</i>
Tree	query-last-member-interval
Range	1 to 1023
Default	1
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

query-response-interval *number*

Description	Time to wait to receive a response to the IGMP membership query from the host
Context	network-instance name <i>string</i> protocols igmp query-response-interval <i>number</i>
Tree	query-response-interval
Range	1 to 1023
Default	10
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

robust-count *number*

Description	Tune IGMP robustness to allow for expected packet loss.
--------------------	---

The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Context	network-instance name <i>string</i> protocols igmp robust-count <i>number</i>
Tree	robust-count
Range	2 to 10
Default	2
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

ssm

Description	Container to configure Source specific multicast (SSM) options.
Context	network-instance name <i>string</i> protocols igmp ssm
Tree	ssm
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

mappings

Description	A list of source specific multicast (SSM) mappings.
Context	network-instance name <i>string</i> protocols igmp ssm mappings
Tree	mappings
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group-range [start string end string](#)

Description	A Source Specific Multicast (SSM) mapping. This allows IGMP v2 hosts to be able to join in SSM environments by translating IGMP v2 reports into IGMP v3 reports. The request in an IGMP v2 join is sent toward the source address found by matching the multicast address.
Context	network-instance name <i>string</i> protocols igmp ssm mappings group-range start string end string
Tree	group-range

Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

start string

Description	Start of the group range.
Context	network-instance name string protocols igmp ssm mappings group-range start string end string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

end string

Description	End of the group range.
Context	network-instance name string protocols igmp ssm mappings group-range start string end string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source [source string](#)

Description	Multicast source address list.
Context	network-instance name string protocols igmp ssm mappings group-range start string end string source source string
Tree	source
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10
Min. Elements	1

source string

Description	Multicast source address.
Context	network-instance name string protocols igmp ssm mappings group-range start string end string source source string
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

trace-options

Description Enter the trace-options context

Context [network-instance name](#) *string* [protocols igmp trace-options](#)

Tree [trace-options](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

trace

Description Tracing parameter flags

Context [network-instance name](#) *string* [protocols igmp trace-options trace](#)

Tree [trace](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interface

Description Enable tracing interface events.

Context [network-instance name](#) *string* [protocols igmp trace-options trace interface](#)

Tree [interface](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

all

Description Trace for all interfaces.

Context [network-instance name](#) *string* [protocols igmp trace-options trace interface all](#)

Tree [all](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *reference*

Description	Trace for interface with this name.
Context	network-instance name <i>string</i> protocols igmp trace-options trace interface name <i>reference</i>
Tree	name
Reference	network-instance name <i>string</i> protocols igmp interface interface-name <i>reference</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

packet

Description	Trace IGMP Packet types Only one type can be enabled at a time
Context	network-instance name <i>string</i> protocols igmp trace-options trace packet
Tree	packet
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interface

Description	Enable interface filter for packets.
Context	network-instance name <i>string</i> protocols igmp trace-options trace packet interface
Tree	interface
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

all

Description	Trace for all interfaces.
Context	network-instance name <i>string</i> protocols igmp trace-options trace packet interface all
Tree	all
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *reference*

Description Trace for interface with this name.

Context [network-instance name](#) *string* [protocols igmp](#) [trace-options](#) [trace packet](#) [interface name](#) *reference*

Tree [name](#)

Reference [network-instance name](#) *string* [protocols igmp](#) [interface interface-name](#) *reference*

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

modifier *keyword*

Description Enter the modifier context

Context [network-instance name](#) *string* [protocols igmp](#) [trace-options](#) [trace packet](#) [modifier](#) *keyword*

Tree [modifier](#)

Default egress-ingress-and-dropped

Options

- dropped
Enable tracing for the packets which are dropped.
- ingress-and-dropped
Enable tracing for the packets which are sent or received.
- egress-ingress-and-dropped
Enable tracing for the packets which are sent, received or dropped.

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

type *keyword*

Description Enter the type context

Context [network-instance name](#) *string* [protocols igmp](#) [trace-options](#) [trace packet](#) [type](#) *keyword*

Tree [type](#)

Options	<ul style="list-style-type: none"> • all Enable tracing of all IGMP packets • query Enable tracing of IGMP Query packets • v1-report Enable tracing of IGMP version 1 Report packets • v2-report Enable tracing of IGMP version 2 Report packets • v2-leave Enable tracing of IGMP version 2 Leave packets • v3-report Enable tracing of IGMP version 3 Report packets
----------------	--

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

isis

Description	Enable the isis context
Context	network-instance name string protocols isis
Tree	isis
Configurable	True
Platforms	Supported on all platforms

instance [name string](#)

Description	List of IS-IS protocol instances associated with this network-instance. Only a single instance is supported for now
Context	network-instance name string protocols isis instance name string
Tree	instance
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

name [string](#)

Description	The name of the IS-IS instance
--------------------	--------------------------------

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Used to administratively enable or disable the IS-IS instance
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

attached-bit

Description	This container provides option for handling the ATTached bit in L1 LSPs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> attached-bit
Tree	attached-bit
Configurable	True
Platforms	Supported on all platforms

ignore *boolean*

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.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> attached-bit ignore <i>boolean</i>
Tree	ignore
Default	false
Configurable	True
Platforms	Supported on all platforms

suppress *boolean*

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.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> attached-bit suppress <i>boolean</i>
Tree	suppress
Default	false
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container for specifying authentication options that apply to the entire IS-IS instance or to an entire level. The settings in this container only apply to PDUs without an authentication behavior specified at a more granular level.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

csnp-authentication

Description	Container with options to control the authentication of CSNP PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication csnp-authentication
Tree	csnp-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication csnp-authentication check-received <i>keyword</i>
Tree	check-received

Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication csnp-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

hello-authentication

Description	Container with options to control the authentication of Hello PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication hello-authentication
Tree	hello-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication hello-authentication check-received <i>keyword</i>

Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication hello-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

key

Description	Container to specify the secret key and crypto algorithm to use for the authentication of PDUs when the behavior is controlled at this level of the configuration hierarchy
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication key
Tree	key
Configurable	True
Platforms	Supported on all platforms

auth-password *string*

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.

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication key auth-password <i>string</i>
Tree	auth-password
String Length	1 to 25
Configurable	True
Platforms	Supported on all platforms

crypto-algorithm *keyword*

Description	The cryptographic algorithm used with the keying material to secure the messages.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication key crypto-algorithm <i>keyword</i>
Tree	crypto-algorithm
Options	<ul style="list-style-type: none"> cleartext The authentication-key is encoded in plaintext. hmac-md5 The authentication-key is used to generate a 16-byte (128 bit) MD5 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).
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Specifies a keychain to use for the authentication of PDUs when the behavior is controlled at this level of the configuration hierarchy.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication keychain <i>reference</i>

Tree	keychain
Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

Isp-authentication

Description	Container with options to control the authentication of Link State PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication lsp-authentication
Tree	lsp-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication lsp-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication lsp-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

psnp-authentication

Description	Container with options to control the authentication of PSNP PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication psnp-authentication
Tree	psnp-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication psnp-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> authentication psnp-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

auto-cost

Description	Enter the auto-cost context
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> auto-cost
Tree	auto-cost
Configurable	True
Platforms	Supported on all platforms

reference-bandwidth *number*

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: $\text{cost} = \text{reference-bandwidth} / \text{bandwidth}$</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>
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> auto-cost reference-bandwidth <i>number</i>
Tree	reference-bandwidth
Range	1 to 8000000000
Units	kbps
Configurable	True
Platforms	Supported on all platforms

export-policy *reference*

Description	Apply an export policy to redistribute non-ISIS routes into ISIS
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> export-policy <i>reference</i>
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

graceful-restart

Description	Container for options related to IS-IS graceful restart
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> graceful-restart
Tree	graceful-restart
Configurable	True
Platforms	Supported on all platforms

helper-mode *boolean*

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.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> graceful-restart helper-mode <i>boolean</i>
Tree	helper-mode
Default	false
Configurable	True
Platforms	Supported on all platforms

hostnames

Description	Enter the hostnames context
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> hostnames
Tree	hostnames
Configurable	False
Platforms	Supported on all platforms

system-id *host-system-id string*

Description	List of system IDs that have discovered hostnames.
Context	network-instance name string protocols isis instance name string hostnames system-id host-system-id string
Tree	system-id
Configurable	False
Platforms	Supported on all platforms

host-system-id *string*

Description	The system ID
Context	network-instance name string protocols isis instance name string hostnames system-id host-system-id string
String Length	14
Configurable	False
Platforms	Supported on all platforms

hostname *string*

Description	The hostname of the system.
Context	network-instance name string protocols isis instance name string hostnames system-id host-system-id string hostname string
Tree	hostname
Configurable	False
Platforms	Supported on all platforms

inter-level-propagation-policies

Description	Container with options to control the propagation of prefixes between levels
Context	network-instance name string protocols isis instance name string inter-level-propagation-policies
Tree	inter-level-propagation-policies
Configurable	True
Platforms	Supported on all platforms

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.
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
Configurable	True
Platforms	Supported on all platforms

summary-address [ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*)

Description	List of summarization prefixes
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</i> <i>ipv6-prefix</i>)
Tree	summary-address
Configurable	True
Platforms	Supported on all platforms

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	An IP prefix advertised into L2 that summarizes one or more L1 prefixes and causes them to be suppressed
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</i> <i>ipv6-prefix</i>)
Configurable	True
Platforms	Supported on all platforms

route-tag *number*

Description	Specifies route tag value to assign to the summary route
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</i> <i>ipv6-prefix</i>) route-tag <i>number</i>
Tree	route-tag
Range	1 to 4294967295
Configurable	True

Platforms Supported on all platforms

interface [interface-name](#) *reference*

Description List of IS-IS interfaces

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference*

Tree [interface](#)

Configurable True

Platforms Supported on all platforms

interface-name *reference*

Description Reference to a specific subinterface of the form <interface-name>.<subinterface-index>

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference*

Reference [network-instance name](#) *string* [interface name](#) *string*

Configurable True

Platforms Supported on all platforms

adjacency [neighbor-system-id](#) *string* [adjacency-level](#) *string*

Description List of adjacencies formed through this interface.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [adjacency neighbor-system-id](#) *string* [adjacency-level](#) *string*

Tree [adjacency](#)

Configurable False

Platforms Supported on all platforms

neighbor-system-id *string*

Description The neighbor router's system ID.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [adjacency neighbor-system-id](#) *string* [adjacency-level](#) *string*

String Length 14

Configurable False

Platforms Supported on all platforms

adjacency-level *string*

Description The level of the adjacency that is formed.

Context [network-instance name *string*](#) [protocols isis instance name *string*](#) [interface interface-name *reference*](#) [adjacency neighbor-system-id *string*](#) [adjacency-level *string*](#)

Configurable False

Platforms Supported on all platforms

down-reason *keyword*

Description The reason why the adjacency is down.

Context [network-instance name *string*](#) [protocols isis instance name *string*](#) [interface interface-name *reference*](#) [adjacency neighbor-system-id *string*](#) [adjacency-level *string*](#) [down-reason *keyword*](#)

Tree [down-reason](#)

Options

- 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

Platforms Supported on all platforms

last-up-down-transition *string*

Description	The last time when the adjacency entered the up or down state.
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> last-up-down-transition <i>string</i>
Tree	last-up-down-transition
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

neighbor-circuit-type *keyword*

Description	The circuit type signalled by the neighbor.
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-circuit-type <i>keyword</i>
Tree	neighbor-circuit-type
Default	L1L2
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	False
Platforms	Supported on all platforms

neighbor-hostname *string*

Description	The hostname of the neighbor, as learned by TLV 137.
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
Configurable	False
Platforms	Supported on all platforms

neighbor-ipv4 *string*

Description	The IPv4 address of the neighbor.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string neighbor-ipv4</i> <i>string</i>
Tree	neighbor-ipv4
Configurable	False
Platforms	Supported on all platforms

neighbor-ipv6 *string*

Description	The IPv6 address of the neighbor.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string neighbor-ipv6</i> <i>string</i>
Tree	neighbor-ipv6
Configurable	False
Platforms	Supported on all platforms

neighbor-last-restart (*keyword* | *date-and-time-delta*)

Description	The last time the neighbor restarted under protection of graceful restart.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string neighbor-last-restart</i> (<i>keyword</i> <i>date-and-time-delta</i>)
Tree	neighbor-last-restart
String Length	20 to 32
Options	<ul style="list-style-type: none"> • never
Configurable	False
Platforms	Supported on all platforms

neighbor-priority *number*

Description	The priority signalled by the neighbor to become the DIS on a LAN
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string neighbor-priority</i> <i>number</i>
Tree	neighbor-priority

Range	0 to 127
Configurable	False
Platforms	Supported on all platforms

neighbor-restart-capable *boolean*

Description	Reads true when the neighbor has signalled that it is restart capable.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string</i> adjacency-level <i>string</i> neighbor-restart-capable <i>boolean</i>
Tree	neighbor-restart-capable
Configurable	False
Platforms	Supported on all platforms

neighbor-restart-status *keyword*

Description	The status of the neighbor with respect to graceful restart
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string</i> adjacency-level <i>string</i> neighbor-restart-status <i>keyword</i>
Tree	neighbor-restart-status
Options	<ul style="list-style-type: none"> • not-helping • helping
Configurable	False
Platforms	Supported on all platforms

neighbor-restarts *number*

Description	The number of times the neighbor has restarted under protection of graceful restart.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string</i> adjacency-level <i>string</i> neighbor-restarts <i>number</i>
Tree	neighbor-restarts
Configurable	False
Platforms	Supported on all platforms

neighbor-snpa *string*

Description	The SNPA of the neighbor.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string neighbor-snpa</i> <i>string</i>
Tree	neighbor-snpa
String Length	0 to 20
Configurable	False
Platforms	Supported on all platforms

remaining-holdtime *number*

Description	The time remaining until the hold timer will expire.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string remaining-holdtime</i> <i>number</i>
Tree	remaining-holdtime
Units	seconds
Configurable	False
Platforms	Supported on all platforms

state *keyword*

Description	The current state of the adjacency.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference adjacency neighbor-system-id</i> <i>string adjacency-level</i> <i>string state</i> <i>keyword</i>
Tree	state
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
Platforms	Supported on all platforms

up-down-transitions *number*

Description	The total number of transitions from Up state to a lower state, since the last clear.
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
Default	0
Configurable	False
Platforms	Supported on all platforms

admin-state *keyword*

Description	Used to administratively enable or disable the IS-IS protocol on a routed subinterface
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
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container for specifying authentication options that apply to the IS-IS instance.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

hello-authentication

Description	Container with options to control the authentication of Hello PDUs
--------------------	--

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication hello-authentication
Tree	hello-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication hello-authentication check-received keyword
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication hello-authentication generate boolean
Tree	generate
Configurable	True
Platforms	Supported on all platforms

key

Description	Container to specify the secret key and crypto algorithm to use for the authentication of Hello PDUs on this interface
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication key
Tree	key
Configurable	True
Platforms	Supported on all platforms

auth-password *string*

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.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication key auth-password <i>string</i>
Tree	auth-password
String Length	1 to 25
Configurable	True
Platforms	Supported on all platforms

crypto-algorithm *keyword*

Description	The cryptographic algorithm used with the keying material to secure the messages.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> authentication key crypto-algorithm <i>keyword</i>
Tree	crypto-algorithm
Options	<ul style="list-style-type: none"> cleartext The authentication-key is encoded in plaintext. hmac-md5 The authentication-key is used to generate a 16-byte (128 bit) MD5 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).

Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Specifies a keychain to use for the authentication of Hello PDUs on this interface.
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
Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

circuit-id *number*

Description	The circuit ID assigned by this IS-IS router to its interface.
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
Configurable	False
Platforms	Supported on all platforms

circuit-type *keyword*

Description	Specifies the circuit type as either point-to-point or broadcast
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
Options	<ul style="list-style-type: none"> • point-to-point This enum describes a point-to-point interface • broadcast This enum describes a broadcast interface
Configurable	True

Platforms Supported on all platforms

hello-padding *keyword*

Description Specifies the use of IS-IS Hello PDU padding on the interface

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [hello-padding](#) *keyword*

Tree [hello-padding](#)

Default disable

Options

- 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

Platforms Supported on all platforms

ipv4-unicast

Description Enter the ipv4-unicast context

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [ipv4-unicast](#)

Tree [ipv4-unicast](#)

Configurable True

Platforms Supported on all platforms

admin-state *keyword*

Description	When set to true, the interface and level supports IPv4 unicast routing
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ipv4-unicast admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

enable-bfd *boolean*

Description	Enable BFD for IPv4
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
Default	false
Configurable	True
Platforms	Supported on all platforms

include-bfd-tlv *boolean*

Description	Specifies whether a BFD-enabled TLV is included for IPv4 on this IS-IS interface.
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
Default	false
Configurable	True
Platforms	Supported on all platforms

ipv6-unicast

Description	Enter the ipv6-unicast context
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
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	When set to true, the interface and level supports IPv6 unicast routing
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
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

enable-bfd *boolean*

Description	Enable BFD for IPv6
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
Default	false
Configurable	True
Platforms	Supported on all platforms

include-bfd-tlv *boolean*

Description	Specifies whether a BFD-enabled TLV is included for IPv6 on this IS-IS interface.
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
Default	false
Configurable	True
Platforms	Supported on all platforms

ldp-synchronization

Description	Container with configuration options and state that pertains to the operation of LDP-IGP synchronization on this interface.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ldp-synchronization
Tree	ldp-synchronization
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

disable

Description	Disable LDP-IGP synchronization procedures on this interface, even if synchronization is enabled globally
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ldp-synchronization disable
Tree	disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

duration *number*

Description	The length of time that the IGP interface has been in sync or out of sync
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ldp-synchronization duration <i>number</i>
Tree	duration
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

end-of-lib *boolean*

Description	<p>When set to true, the IGP restores the normal metric for the IGP adjacency when learning from LDP that all label-FEC mappings have been received from the LDP peer, even if there is remaining time on the hold-down-timer.</p> <p>When set to false, the IGP always waits for the full duration of the hold-down-timer to restore the normal metric for the IGP adjacency.</p> <p>This overrides the global/instance level setting.</p>
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ldp-synchronization end-of-lib <i>boolean</i>

Tree	end-of-lib
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hold-down-timer *number*

Description	The maximum amount of time that the IGP advertises a maximum metric for an interface, measured from the time that the LDP adjacency is re-established after going down. This overrides the global/instance level setting.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ldp-synchronization hold-down-timer <i>number</i>
Tree	hold-down-timer
Range	1 to 1800
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

sync-state *keyword*

Description	The current state of the interface with respect to LDP-IGP sync
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> ldp-synchronization sync-state <i>keyword</i>
Tree	sync-state
Options	<ul style="list-style-type: none"> • wait-for-LDP-adjacency The IGP is waiting for the LDP adjacency to come up. The interface is being advertised with max-metric. • hold-down-timer-active The LDP adjacency has come up and the IGP has started the hold-down-timer, waiting for either end-of-lib or hold-down-timer expiry. The interface is being advertised with max-metric. • end-of-lib-received The IGP received end-of-lib and has switched to normal operation. The interface is being advertised with a normal metric • hold-down-timer-expired The IGP did not receive end-of-lib (or was configured to ignore it) but hold-down-timer has expired and normal metric is restored. • manual-exit

A tools command was performed to exit ldp-sync. Normal operation is resumed, max-metric is removed.

- disabled

ldp-sync is not applicable on this interface

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

level *level-number number*

Description	List of IS-IS levels supported by this interface
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference level level-number number</i>
Tree	level
Configurable	True
Platforms	Supported on all platforms
Max. Elements	2

level-number *number*

Description	Specifies the IS-IS protocol level to which these attributes are applied.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference level level-number number</i>
Range	1 to 2
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container for specifying authentication options that apply to the IS-IS instance.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference level level-number number authentication</i>
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

hello-authentication

Description	Container with options to control the authentication of Hello PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference level level-number</i> <i>number</i> authentication hello-authentication
Tree	hello-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference level level-number</i> <i>number</i> authentication hello-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference level level-number</i> <i>number</i> authentication hello-authentication generate <i>boolean</i>
Tree	generate

Configurable	True
Platforms	Supported on all platforms

key

Description	Container to specify the secret key and crypto algorithm to use for the authentication of Hello PDUs on this interface
Context	network-instance name string protocols isis instance name string interface interface-name reference level level-number number authentication key
Tree	key
Configurable	True
Platforms	Supported on all platforms

auth-password *string*

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.
Context	network-instance name string protocols isis instance name string interface interface-name reference level level-number number authentication key auth-password string
Tree	auth-password
String Length	1 to 25
Configurable	True
Platforms	Supported on all platforms

crypto-algorithm *keyword*

Description	The cryptographic algorithm used with the keying material to secure the messages.
Context	network-instance name string protocols isis instance name string interface interface-name reference level level-number number authentication key crypto-algorithm keyword
Tree	crypto-algorithm

Options	<ul style="list-style-type: none"> cleartext The authentication-key is encoded in plaintext. hmac-md5 The authentication-key is used to generate a 16-byte (128 bit) MD5 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).
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Specifies a keychain to use for the authentication of Hello PDUs on this interface.
Context	network-instance name string protocols isis instance name string interface interface-name reference level level-number number authentication keychain reference
Tree	keychain
Reference	system authentication keychain name string
Configurable	True
Platforms	Supported on all platforms

disable *boolean*

Description	Disable the Level for the interface.
Context	network-instance name string protocols isis instance name string interface interface-name reference level level-number number disable boolean
Tree	disable
Default	false
Configurable	True
Platforms	Supported on all platforms

ipv6-unicast-metric *number*

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.
--------------------	---

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 number
Tree	ipv6-unicast-metric
Range	1 to 16777215
Configurable	True
Platforms	Supported on all platforms

metric number

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.
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 number
Tree	metric
Range	1 to 16777215
Configurable	True
Platforms	Supported on all platforms

priority number

Description	ISIS neighbor priority for becoming Designated IS (LAN hello PDU only).
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 number
Tree	priority
Range	0 to 127
Default	64
Configurable	True
Platforms	Supported on all platforms

timers

Description	Enter the timers context
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
Configurable	True

Platforms Supported on all platforms

hello-interval *number*

Description ISIS hello-interval value. The default is 3 seconds on Designated IS interfaces and 9 seconds for non-DIS and p2p interfaces

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [level level-number](#) *number* [timers hello-interval number](#)

Tree [hello-interval](#)

Range 1 to 20000

Default 9

Units seconds

Configurable True

Platforms Supported on all platforms

hello-multiplier *number*

Description ISIS hello-multiplier value.

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.

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.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [level level-number](#) *number* [timers hello-multiplier number](#)

Tree [hello-multiplier](#)

Range 2 to 100

Default 3

Configurable True

Platforms Supported on all platforms

oper-state *keyword*

Description The operational state of the IS-IS interface. This simply tracks the operational state of the subinterface.

Context	<code>network-instance name</code> <i>string</i> <code>protocols isis instance name</code> <i>string</i> <code>interface interface-name</code> <i>reference</i> <code>oper-state</code> <i>keyword</i>
Tree	<code>oper-state</code>
Options	<ul style="list-style-type: none"> • <code>up</code> Component or process is operational • <code>down</code> Component or process is not operational • <code>empty</code> Component slot is empty • <code>downloading</code> Component is downloading image into memory • <code>booting</code> Component is booting downloaded image • <code>starting</code> Component image operational, application processes starting • <code>failed</code> Component or process has failed • <code>synchronizing</code> Component is currently being synchronized • <code>upgrading</code> Component is currently being upgraded • <code>low-power</code> Component is offline due to insufficient system power • <code>degraded</code> Component or process is in a degraded state • <code>warm-reboot</code> Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • <code>waiting</code> Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the <code>reinvoke-with-delay</code> action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False

Platforms Supported on all platforms

passive *boolean*

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.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [passive](#) *boolean*

Tree [passive](#)

Default false

Configurable True

Platforms Supported on all platforms

segment-routing

Description Container with interface-specific segment routing options

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [segment-routing](#)

Tree [segment-routing](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

mpls

Description SR-MPLS interface options

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [segment-routing mpls](#)

Tree [mpls](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

ipv4-node-sid

Description Configuration of IPv4 node SID.
The (primary) IPv4 address of this interface is advertised as a prefix SID with the node-SID flag set. The associated label is derived from the label index configured in this container.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [interface interface-name](#) *reference* [segment-routing mpls ipv4-node-sid](#)

Tree	ipv4-node-sid
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

index number

Description	Label index to add to SRGB base. This causes the V-flag and L-flag in the prefix SID subTLV to be set to zero.
Context	network-instance name string protocols isis instance name string interface interface-name reference segment-routing mpls ipv4-node-sid index number
Tree	index
Range	0 to 1048575
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-node-sid

Description	Configuration of IPv6 node SID. The (primary) IPv6 address of this interface is advertised as a prefix SID with the node-SID flag set. The associated label is derived from the label index configured in this container.
Context	network-instance name string protocols isis instance name string interface interface-name reference segment-routing mpls ipv6-node-sid
Tree	ipv6-node-sid
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

index number

Description	Label index to add to SRGB base. This causes the V-flag and L-flag in the prefix SID subTLV to be set to zero.
Context	network-instance name string protocols isis instance name string interface interface-name reference segment-routing mpls ipv6-node-sid index number
Tree	index
Range	0 to 1048575
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

timers

Description	Enter the timers context
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> timers
Tree	timers
Configurable	True
Platforms	Supported on all platforms

csnp-interval *number*

Description	The interval, specified in seconds, at which periodic CSNP packets should be transmitted by the local IS on this interface.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> timers csnp-interval <i>number</i>
Tree	csnp-interval
Range	1 to 65535
Default	10
Units	seconds
Configurable	True
Platforms	Supported on all platforms

lsp-pacing-interval *number*

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>
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
Range	0 to 100000
Default	100

Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

trace-options

Description	Interface level debug trace options for IS-IS
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
Configurable	True
Platforms	Supported on all platforms

trace *keyword*

Description	List of tracing options
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> interface interface-name <i>reference</i> trace-options trace keyword
Tree	trace
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
Platforms	Supported on all platforms

ipv4-unicast

Description	Enables/disables IPv4 routing in this ISIS instance.
--------------------	--

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ipv4-unicast
Tree	ipv4-unicast
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	When set to true, the IS-IS instance supports IPv4 unicast routing
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ipv4-unicast admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

ipv6-unicast

Description	Enables/disables IPv6 routing in this ISIS instance.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ipv6-unicast
Tree	ipv6-unicast
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	When set to true, the IS-IS instance supports IPv6 unicast routing
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ipv6-unicast admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True

Platforms Supported on all platforms

multi-topology *boolean*

Description When set to true, IS-IS multi-topology TLVs are used for IPv6 routing and support for native IPv6 TLVs is disabled.

Context [network-instance name string protocols isis instance name string ipv6-unicast multi-topology boolean](#)

Tree [multi-topology](#)

Default false

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

ldp-synchronization

Description Enable LDP-IGP synchronization procedures on all P2P interfaces and all LAN interfaces with a single adjacency, except on interfaces where the functionality is explicitly disabled.

Context [network-instance name string protocols isis instance name string ldp-synchronization](#)

Tree [ldp-synchronization](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

end-of-lib *boolean*

Description When set to true, the IGP restores the normal metric for the IGP adjacency when learning from LDP that all label-FEC mappings have been received from the LDP peer, even if there is remaining time on the hold-down-timer. When set to false, the IGP always waits for the full duration of the hold-down-timer to restore the normal metric for the IGP adjacency.

Context [network-instance name string protocols isis instance name string ldp-synchronization end-of-lib boolean](#)

Tree [end-of-lib](#)

Default false

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

hold-down-timer *number*

Description	The maximum amount of time that the IGP advertises a maximum metric for an interface, measured from the time that the LDP adjacency is re-established after going down.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> ldp-synchronization hold-down-timer <i>number</i>
Tree	hold-down-timer
Range	1 to 1800
Default	60
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

level [level-number](#) *number*

Description	List of IS-IS levels supported by this IS (router)
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i>
Tree	level
Configurable	True
Platforms	Supported on all platforms
Max. Elements	2

level-number *number*

Description	Specifies the IS-IS protocol level to which these attributes are applied.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i>
Range	1 to 2
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container for specifying authentication options that apply to the entire IS-IS instance or to an entire level. The settings in this container only apply to PDUs without an authentication behavior specified at a more granular level.
--------------------	--

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

csnp-authentication

Description	Container with options to control the authentication of CSNP PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication csnp-authentication
Tree	csnp-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication csnp-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication csnp-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

hello-authentication

Description	Container with options to control the authentication of Hello PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication hello-authentication
Tree	hello-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication hello-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication hello-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

key

Description	Container to specify the secret key and crypto algorithm to use for the authentication of PDUs when the behavior is controlled at this level of the configuration hierarchy
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication key
Tree	key
Configurable	True
Platforms	Supported on all platforms

auth-password *string*

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.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication key auth-password <i>string</i>
Tree	auth-password
String Length	1 to 25
Configurable	True
Platforms	Supported on all platforms

crypto-algorithm *keyword*

Description	The cryptographic algorithm used with the keying material to secure the messages.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication key crypto-algorithm <i>keyword</i>
Tree	crypto-algorithm
Options	<ul style="list-style-type: none"> cleartext The authentication-key is encoded in plaintext. hmac-md5 The authentication-key is used to generate a 16-byte (128 bit) MD5 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).
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Specifies a keychain to use for the authentication of PDUs when the behavior is controlled at this level of the configuration hierarchy.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication keychain <i>reference</i>
Tree	keychain
Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

Isp-authentication

Description	Container with options to control the authentication of Link State PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication Isp-authentication
Tree	Isp-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication lsp-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication lsp-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

psnp-authentication

Description	Container with options to control the authentication of PSNP PDUs
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication psnp-authentication
Tree	psnp-authentication
Configurable	True
Platforms	Supported on all platforms

check-received *keyword*

Description	Specifies the type of authentication checks done for received PDUs of the specified type.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication psnp-authentication check-received <i>keyword</i>
Tree	check-received
Options	<ul style="list-style-type: none"> • strict Strict authentication option. Reject all packets that do not have an authentication TLV or that do have an authentication TLV that cannot be validated. • loose Loose authentication option. Accept packets received without an authentication TLV; validate packets received with an authentication TLV and reject those packets that cannot be validated. • disable This enum disables authentication checks. Do not check authentication TLV (if any) of received PDUs; authentication TLV may still be added self-generated PDUs
Configurable	True
Platforms	Supported on all platforms

generate *boolean*

Description	When set to true, IS-IS is instructed to add an authentication TLV to every transmitted PDU of the specified type
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> level level-number <i>number</i> authentication psnp-authentication generate <i>boolean</i>
Tree	generate
Configurable	True
Platforms	Supported on all platforms

metric-style *keyword*

Description	Specifies the metric style to be wide or narrow for the level
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
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
Platforms	Supported on all platforms

route-preference

Description	Specify the route preference (admin distance) for IP routes associated with the level
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
Configurable	True
Platforms	Supported on all platforms

external *number*

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.
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
Range	1 to 255
Configurable	True
Platforms	Supported on all platforms

internal *number*

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.
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
Range	1 to 255
Configurable	True

Platforms Supported on all platforms

trace-options

Description Level debug trace options for IS-IS

Context [network-instance name string protocols isis instance name string level level-number number trace-options](#)

Tree [trace-options](#)

Configurable True

Platforms Supported on all platforms

trace keyword

Description List of tracing options

Context [network-instance name string protocols isis instance name string level level-number number trace-options trace keyword](#)

Tree [trace](#)

Options

- adjacencies
- lsdb
- routes
- spf

Configurable True

Platforms Supported on all platforms

level-capability keyword

Description The level-capability of the intermediate system (router)

Context [network-instance name string protocols isis instance name string level-capability keyword](#)

Tree [level-capability](#)

Default L2

Options

- L1
This enum describes ISIS level 1
- L2
This enum describes ISIS level 2
- L1L2
This enum describes ISIS level 1-2

Configurable	True
Platforms	Supported on all platforms

level-database *level-number number lsp-id string*

Description	Link State database
Context	network-instance name string protocols isis instance name string level-database level-number number lsp-id string
Tree	level-database
Configurable	False
Platforms	Supported on all platforms

level-number *number*

Description	Specifies the IS-IS protocol level to which these attributes are applied.
Context	network-instance name string protocols isis instance name string level-database level-number number lsp-id string
Range	1 to 2
Configurable	False
Platforms	Supported on all platforms

lsp-id *string*

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.
Context	network-instance name string protocols isis instance name string level-database level-number number lsp-id string
String Length	20
Configurable	False
Platforms	Supported on all platforms

attributes

Description	Enter the attributes context
Context	network-instance name string protocols isis instance name string level-database level-number number lsp-id string attributes
Tree	attributes
Configurable	False

Platforms Supported on all platforms

attached *boolean*

Description Set to true in the L1 LSP when the IS has a Level 2 adjacency.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [attributes attached](#) *boolean*

Tree [attached](#)

Configurable False

Platforms Supported on all platforms

level1-is-type *boolean*

Description Set to true when the router participates in L1

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [attributes level1-is-type](#) *boolean*

Tree [level1-is-type](#)

Configurable False

Platforms Supported on all platforms

level2-is-type *boolean*

Description Set to true when the router participates in L2

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [attributes level2-is-type](#) *boolean*

Tree [level2-is-type](#)

Configurable False

Platforms Supported on all platforms

overload *boolean*

Description Set to true when the IS is in overload state and should be avoided for transit.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [attributes overload](#) *boolean*

Tree [overload](#)

Configurable False

Platforms Supported on all platforms

checksum *string*

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.
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
Configurable	False
Platforms	Supported on all platforms

defined-tlvs

Description	List of defined TLV-s contained in LSP.
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
Configurable	False
Platforms	Supported on all platforms

area-addresses *string*

Description	Each item represents an area address advertised by the LSP.
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
String Length	2 to 38
Configurable	False
Platforms	Supported on all platforms

authentication

Description	Authentication TLV. TLV type = 10
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
Configurable	False

Platforms Supported on all platforms

auth-data *string*

Description The authentication data

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs authentication auth-data](#) *string*

Tree [auth-data](#)

Configurable False

Platforms Supported on all platforms

auth-type *keyword*

Description Enter the auth-type context

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs authentication auth-type](#) *keyword*

Tree [auth-type](#)

Options

- cleartext
- crypto
- hmac-md5

Configurable False

Platforms Supported on all platforms

extended-ipv4-reachability [ipv4-prefix](#) *string*

Description TLV specifying extended IPv4 Reachability information in the LSP. TLV type = 135

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs extended-ipv4-reachability ipv4-prefix](#) *string*

Tree [extended-ipv4-reachability](#)

Configurable False

Platforms Supported on all platforms

ipv4-prefix *string*

Description An IPv4 prefix that is reachable to the router.

Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs extended-ipv4-reachability ipv4-prefix string</code>
Configurable	False
Platforms	Supported on all platforms

down *boolean*

Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs extended-ipv4-reachability ipv4-prefix string down boolean</code>
Tree	<code>down</code>
Configurable	False
Platforms	Supported on all platforms

metric *number*

Description	The default metric to reach the IPv4 prefix.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs extended-ipv4-reachability ipv4-prefix string metric number</code>
Tree	<code>metric</code>
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

sub-tlvs

Description	SubTLVs of TLV 135, TLV 235, TLV 236 and TLV 237
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs extended-ipv4-reachability ipv4-prefix string sub-tlvs</code>
Tree	<code>sub-tlvs</code>
Configurable	False
Platforms	Supported on all platforms

route-tag-32bit *number*

Description	List of 32-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-32bit <i>number</i>
Tree	route-tag-32bit
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

route-tag-64bit *number*

Description	List of 64-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-64bit <i>number</i>
Tree	route-tag-64bit
Configurable	False
Platforms	Supported on all platforms

segment-routing-prefix-sid

Description	Carries a segment routing prefix SID
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> sub-tlvs segment-routing-prefix-sid
Tree	segment-routing-prefix-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

algorithm *keyword*

Description	Contains the identifier of the algorithm the router uses to compute the reachability of the prefix to which the Prefix-SID is associated
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> sub-tlvs segment-routing-prefix-sid algorithm <i>keyword</i>
Tree	algorithm

Options	<ul style="list-style-type: none"> • spf • strict-spf
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

explicit-null *boolean*

Description	If set any upstream neighbor of the Prefix-SID originator MUST replace the Prefix-SID with a Prefix-SID that has an Explicit NULL value (0 for IPv4 and 2 for IPv6) before forwarding the packet
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> sub-tlvs segment-routing-prefix-sid explicit-null <i>boolean</i>
Tree	explicit-null
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Prefix-SID has local significance.
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> sub-tlvs segment-routing-prefix-sid local <i>boolean</i>
Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

node-sid *boolean*

Description	If set the prefix SID refers to the router identified by the prefix.
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> sub-tlvs segment-routing-prefix-sid node-sid <i>boolean</i>
Tree	node-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

penultimate-hop-popping *boolean*

Description	If set the penultimate hop MUST NOT pop the Prefix-SID before delivering the packet to the node that advertised the Prefix-SID.
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> sub-tlvs segment-routing-prefix-sid penultimate-hop-popping <i>boolean</i>
Tree	penultimate-hop-popping
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

re-advertised *boolean*

Description	If set the prefix to which this Prefix-SID is attached has been propagated by the router from either another level or from another protocol.
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> sub-tlvs segment-routing-prefix-sid re-advertised <i>boolean</i>
Tree	re-advertised
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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> sub-tlvs segment-routing-prefix-sid sr-index-or-label <i>number</i>
Tree	sr-index-or-label
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Prefix-SID carries a value
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> sub-tlvs segment-routing-prefix-sid <i>value</i> <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

extended-is-reachability [neighbor](#) *string*

Description	Each TLV encodes the identity of an adjacent IS neighbor. TLV type = 22
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
Configurable	False
Platforms	Supported on all platforms

neighbor *string*

Description	An adjacent IS neighbor
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>
String Length	17
Configurable	False
Platforms	Supported on all platforms

default-metric *number*

Description	The default metric to reach this adjacent neighbor.
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
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

sub-tlvs

Description	SubTLVs of TLV 22 and TLV 222
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
Configurable	False
Platforms	Supported on all platforms

ipv4-interface-address *string*

Description	The IPv4 address of the interface to the neighbor. Sub-TLV = 6.
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
Configurable	False
Platforms	Supported on all platforms

ipv4-neighbor-address *string*

Description	The IPv4 address of the neighbor. Sub-TLV = 8.
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-neighbor-address <i>string</i>
Tree	ipv4-neighbor-address
Configurable	False
Platforms	Supported on all platforms

ipv6-interface-address *string*

Description	The IPv6 address of the interface to the neighbor. Sub-TLV = 12.
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 ipv6-interface-address <i>string</i>
Tree	ipv6-interface-address
Configurable	False
Platforms	Supported on all platforms

ipv6-neighbor-address *string*

Description	The IPv4 address of the neighbor. Sub-TLV = 13.
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 ipv6-neighbor-address <i>string</i>
Tree	ipv6-neighbor-address
Configurable	False
Platforms	Supported on all platforms

link-msd

Description	The maximum segment depth of the link to the neighbor. Sub-TLV = 15.
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 link-msd
Tree	link-msd
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-info [msd-type](#) (*keyword* | *number*) [msd-value](#) *number*

Description	List of MSD entries
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 link-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Tree	msd-info
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-type (*keyword* | *number*)

Description	MSD type
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 link-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Range	2 to 254

Options	• base-mpls-imposition-msd
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-value *number*

Description	A number in the range of 0-255 representing the maximum SID depth; for all MSD-Types, 0 represents the lack of ability to support a SID stack of any depth
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 link-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

segment-routing-adjacency-sid [sr-index-or-label](#) *number*

Description	List of Adj-SID sub-TLVs associated with the neighbor. Sub-TLV = 31.
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i>
Tree	segment-routing-adjacency-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

adj-set *boolean*

Description	When set, the S-Flag indicates that the Adj-SID refers to a set of adjacencies.
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> adj-set <i>boolean</i>
Tree	adj-set
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

backup *boolean*

Description	If set, the Adj-SID is eligible for protection
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> backup <i>boolean</i>
Tree	backup
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-family *boolean*

Description	If set, then the Adj-SID is used for forwarding IPv6 traffic to the neighbor; else the Adj-SID is used for forwarding IPv4 traffic.
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> ipv6-family <i>boolean</i>
Tree	ipv6-family
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Adj-SID has local significance.
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> local <i>boolean</i>

Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

persistent *boolean*

Description	When set, the P-Flag indicates that the Adj-SID is persistently allocated, i.e., the Adj-SID value remains consistent across router restart and/or interface flap
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> persistent <i>boolean</i>
Tree	persistent
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Adj-SID carries a value
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> value <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

weight *number*

Description	The value represents the weight of the Adj-SID for the purpose of load balancing
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 segment-routing-adjacency-sid sr-index-or-label <i>number</i> weight <i>number</i>
Tree	weight
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

segment-routing-lan-adjacency-sid sr-index-or-label number

Description	List of LAN Adj-SID sub-TLVs. Each describes the set of Adj-SIDs the router assigned to each of its LAN neighbors. Sub-TLV = 32.
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i>
Tree	segment-routing-lan-adjacency-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label number

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

adj-set boolean

Description	When set, the S-Flag indicates that the Adj-SID refers to a set of adjacencies.
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> adj-set <i>boolean</i>
Tree	adj-set
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

backup boolean

Description	If set, the Adj-SID is eligible for protection
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> backup <i>boolean</i>

Tree	backup
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-family *boolean*

Description	If set, then the Adj-SID is used for forwarding IPv6 traffic to the neighbor; else the Adj-SID is used for forwarding IPv4 traffic.
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> ipv6-family <i>boolean</i>
Tree	ipv6-family
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Adj-SID has local significance.
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> local <i>boolean</i>
Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

neighbor-system-id *string*

Description	IS-IS system-ID of the LAN neighbor
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> neighbor-system-id <i>string</i>
Tree	neighbor-system-id
String Length	14
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

persistent *boolean*

Description	When set, the P-Flag indicates that the Adj-SID is persistently allocated, i.e., the Adj-SID value remains consistent across router restart and/or interface flap
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> persistent <i>boolean</i>
Tree	persistent
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Adj-SID carries a value
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> value <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

weight *number*

Description	The value represents the weight of the Adj-SID for the purpose of load balancing
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 segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> weight <i>number</i>
Tree	weight
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

hostname *string*

Description	Host name that advertised this LSP.
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
Configurable	False
Platforms	Supported on all platforms

ipv4-external-reachability [ipv4-prefix](#) *string*

Description	TLV specifying external IPv4 Reachability information in the LSP. External reachability is typically routing information learned from another protocol. TLV type = 130
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
Configurable	False
Platforms	Supported on all platforms

ipv4-prefix *string*

Description	An IPv4 prefix that is reachable to the router.
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>
Configurable	False
Platforms	Supported on all platforms

default-metric *number*

Description	The default metric to reach the IPv4 prefix.
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
Range	0 to 63
Configurable	False
Platforms	Supported on all platforms

default-metric-type *keyword*

Description	The default metric type: internal or external.
--------------------	--

Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs ipv4-external-reachability ipv4-prefix string default-metric-type keyword</code>
Tree	<code>default-metric-type</code>
Options	<ul style="list-style-type: none"> • <code>internal</code> This enum describes internal route type • <code>external</code> This enum describes external route type
Configurable	False
Platforms	Supported on all platforms

down *boolean*

Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs ipv4-external-reachability ipv4-prefix string down boolean</code>
Tree	<code>down</code>
Configurable	False
Platforms	Supported on all platforms

ipv4-interface-addresses (*ipv4-address | ipv6-address*)

Description	Each item represents an IPv4 address configured on an interface in this IS-IS instance.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs ipv4-interface-addresses (ipv4-address ipv6-address)</code>
Tree	<code>ipv4-interface-addresses</code>
Configurable	False
Platforms	Supported on all platforms

ipv4-internal-reachability *ipv4-prefix string*

Description	TLV specifying internal IPv4 Reachability information in the LSP. TLV type = 128
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs ipv4-internal-reachability ipv4-prefix string</code>

Tree	ipv4-internal-reachability
Configurable	False
Platforms	Supported on all platforms

ipv4-prefix *string*

Description	An IPv4 prefix that is reachable to the router.
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>
Configurable	False
Platforms	Supported on all platforms

default-metric *number*

Description	The default metric to reach the IPv4 prefix.
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
Range	0 to 63
Configurable	False
Platforms	Supported on all platforms

default-metric-type *keyword*

Description	The default metric type: internal or external.
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
Options	<ul style="list-style-type: none"> • <code>internal</code> This enum describes internal route type • <code>external</code> This enum describes external route type
Configurable	False
Platforms	Supported on all platforms

down *boolean*

Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
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
Configurable	False
Platforms	Supported on all platforms

ipv6-interface-addresses (*ipv4-address* | *ipv6-address*)

Description	Each item represents an IPv6 address configured on an interface in this IS-IS instance.
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</i> <i>ipv6-address</i>)
Tree	ipv6-interface-addresses
Configurable	False
Platforms	Supported on all platforms

ipv6-reachability *ipv6-prefix string*

Description	TLV specifying IPv6 Reachability information in the LSP. TLV type = 236
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
Configurable	False
Platforms	Supported on all platforms

ipv6-prefix *string*

Description	An IPv6 prefix that is reachable to the router.
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>
Configurable	False
Platforms	Supported on all platforms

down *boolean*

Description	Reads true when the IPv6 prefix was leaked down from Level2 to Level1.
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
Configurable	False
Platforms	Supported on all platforms

external *boolean*

Description	Reads true when the IPv6 prefix reachability is external (learned from another protocol).
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
Configurable	False
Platforms	Supported on all platforms

metric *number*

Description	The metric to reach this IPv6 prefix.
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
Range	0 to 16777215
Configurable	False
Platforms	Supported on all platforms

sub-tlvs

Description	SubTLVs of TLV 135, TLV 235, TLV 236 and TLV 237
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> sub-tlvs
Tree	sub-tlvs

Configurable	False
Platforms	Supported on all platforms

route-tag-32bit *number*

Description	List of 32-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-32bit <i>number</i>
Tree	route-tag-32bit
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

route-tag-64bit *number*

Description	List of 64-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-64bit <i>number</i>
Tree	route-tag-64bit
Configurable	False
Platforms	Supported on all platforms

segment-routing-prefix-sid

Description	Carries a segment routing prefix SID
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> sub-tlvs segment-routing-prefix-sid
Tree	segment-routing-prefix-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

algorithm *keyword*

Description	Contains the identifier of the algorithm the router uses to compute the reachability of the prefix to which the Prefix-SID is associated
--------------------	--

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> sub-tlvs segment-routing-prefix-sid <i>algorithm</i> <i>keyword</i>
Tree	algorithm
Options	<ul style="list-style-type: none"> • spf • strict-spf
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

explicit-null *boolean*

Description	If set any upstream neighbor of the Prefix-SID originator MUST replace the Prefix-SID with a Prefix-SID that has an Explicit NULL value (0 for IPv4 and 2 for IPv6) before forwarding the packet
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> sub-tlvs segment-routing-prefix-sid explicit-null <i>boolean</i>
Tree	explicit-null
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Prefix-SID has local significance.
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> sub-tlvs segment-routing-prefix-sid local <i>boolean</i>
Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

node-sid *boolean*

Description	If set the prefix SID refers to the router identified by the prefix.
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> sub-tlvs segment-routing-prefix-sid node-sid <i>boolean</i>
Tree	node-sid
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

penultimate-hop-popping *boolean*

Description If set the penultimate hop MUST NOT pop the Prefix-SID before delivering the packet to the node that advertised the Prefix-SID.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs ipv6-reachability ipv6-prefix](#) *string* [sub-tlvs segment-routing-prefix-sid penultimate-hop-popping](#) *boolean*

Tree [penultimate-hop-popping](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

re-advertised *boolean*

Description If set the prefix to which this Prefix-SID is attached has been propagated by the router from either another level or from another protocol.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs ipv6-reachability ipv6-prefix](#) *string* [sub-tlvs segment-routing-prefix-sid re-advertised](#) *boolean*

Tree [re-advertised](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs ipv6-reachability ipv6-prefix](#) *string* [sub-tlvs segment-routing-prefix-sid sr-index-or-label](#) *number*

Tree [sr-index-or-label](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

value *boolean*

Description If set then the Prefix-SID carries a value

Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs ipv6-reachability ipv6-prefix string sub-tlvs segment-routing-prefix-sid value boolean</code>
Tree	<code>value</code>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

is-reachability neighbor string

Description	Each TLV encodes the identity of an adjacent IS neighbor. TLV type = 2
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs is-reachability neighbor string</code>
Tree	<code>is-reachability</code>
Configurable	False
Platforms	Supported on all platforms

neighbor string

Description	An adjacent IS neighbor
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs is-reachability neighbor string</code>
String Length	17
Configurable	False
Platforms	Supported on all platforms

default-metric number

Description	The default metric to reach this adjacent neighbor.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs is-reachability neighbor string default-metric number</code>
Tree	<code>default-metric</code>
Range	0 to 63
Configurable	False
Platforms	Supported on all platforms

default-metric-type *keyword*

Description	The default metric type: internal or external.
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
Options	<ul style="list-style-type: none"> • internal • external
Configurable	False
Platforms	Supported on all platforms

mt-ipv4-reachability [ipv4-prefix](#) *string*

Description	TLV specifying multi-topology IPv4 reachability information in the LSP. TLV type = 235
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
Configurable	False
Platforms	Supported on all platforms

ipv4-prefix *string*

Description	An IPv4 prefix that is reachable to the router.
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>
Configurable	False
Platforms	Supported on all platforms

down *boolean*

Description	Reads true when the IPv4 prefix was leaked down from Level2 to Level1.
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
Configurable	False

Platforms Supported on all platforms

metric number

Description The default metric to reach the IPv4 prefix.

Context [network-instance name string](#) [protocols isis instance name string](#) [level-database level-number number](#) [lsp-id string](#) [defined-tlvs mt-ipv4-reachability ipv4-prefix string](#) [metric number](#)

Tree [metric](#)

Range 1 to 16777215

Configurable False

Platforms Supported on all platforms

mt-id number

Description A multi-topology ID.

Context [network-instance name string](#) [protocols isis instance name string](#) [level-database level-number number](#) [lsp-id string](#) [defined-tlvs mt-ipv4-reachability ipv4-prefix string](#) [mt-id number](#)

Tree [mt-id](#)

Range 0 to 4095

Configurable False

Platforms Supported on all platforms

sub-tlvs

Description SubTLVs of TLV 135, TLV 235, TLV 236 and TLV 237

Context [network-instance name string](#) [protocols isis instance name string](#) [level-database level-number number](#) [lsp-id string](#) [defined-tlvs mt-ipv4-reachability ipv4-prefix string](#) [sub-tlvs](#)

Tree [sub-tlvs](#)

Configurable False

Platforms Supported on all platforms

route-tag-32bit number

Description List of 32-bit administrative tag values associated with the IPv4 prefix.

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> sub-tlvs route-tag-32bit <i>number</i>
Tree	route-tag-32bit
Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

route-tag-64bit *number*

Description	List of 64-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-64bit <i>number</i>
Tree	route-tag-64bit
Configurable	False
Platforms	Supported on all platforms

segment-routing-prefix-sid

Description	Carries a segment routing prefix SID
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> sub-tlvs segment-routing-prefix-sid
Tree	segment-routing-prefix-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

algorithm *keyword*

Description	Contains the identifier of the algorithm the router uses to compute the reachability of the prefix to which the Prefix-SID is associated
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> sub-tlvs segment-routing-prefix-sid algorithm <i>keyword</i>
Tree	algorithm
Options	<ul style="list-style-type: none"> • <code>spf</code> • <code>strict-spf</code>
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

explicit-null *boolean*

Description If set any upstream neighbor of the Prefix-SID originator MUST replace the Prefix-SID with a Prefix-SID that has an Explicit NULL value (0 for IPv4 and 2 for IPv6) before forwarding the packet

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs mt-ipv4-reachability ipv4-prefix](#) *string* [sub-tlvs segment-routing-prefix-sid explicit-null](#) *boolean*

Tree [explicit-null](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

local *boolean*

Description If set, then the value/index carried by the Prefix-SID has local significance.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs mt-ipv4-reachability ipv4-prefix](#) *string* [sub-tlvs segment-routing-prefix-sid local](#) *boolean*

Tree [local](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

node-sid *boolean*

Description If set the prefix SID refers to the router identified by the prefix.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs mt-ipv4-reachability ipv4-prefix](#) *string* [sub-tlvs segment-routing-prefix-sid node-sid](#) *boolean*

Tree [node-sid](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

penultimate-hop-popping *boolean*

Description If set the penultimate hop MUST NOT pop the Prefix-SID before delivering the packet to the node that advertised the Prefix-SID.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [level-database level-number](#) *number* [lsp-id](#) *string* [defined-tlvs mt-ipv4-reachability](#)

	ipv4-prefix <i>string</i> sub-tlvs segment-routing-prefix-sid penultimate-hop-popping <i>boolean</i>
Tree	penultimate-hop-popping
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

re-advertised *boolean*

Description	If set the prefix to which this Prefix-SID is attached has been propagated by the router from either another level or from another protocol.
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> sub-tlvs segment-routing-prefix-sid re-advertised <i>boolean</i>
Tree	re-advertised
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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> sub-tlvs segment-routing-prefix-sid sr-index-or-label <i>number</i>
Tree	sr-index-or-label
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Prefix-SID carries a value
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> sub-tlvs segment-routing-prefix-sid value <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

mt-ipv6-reachability *ipv6-prefix string*

Description	TLV specifying IPv6 Reachability information in the LSP. TLV type = 237
Context	<i>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-ipv6-reachability ipv6-prefix string</i>
Tree	<i>mt-ipv6-reachability</i>
Configurable	False
Platforms	Supported on all platforms

ipv6-prefix *string*

Description	An IPv6 prefix that is reachable to the router.
Context	<i>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-ipv6-reachability ipv6-prefix string</i>
Configurable	False
Platforms	Supported on all platforms

down *boolean*

Description	Reads true when the IPv6 prefix was leaked down from Level2 to Level1.
Context	<i>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-ipv6-reachability ipv6-prefix string down boolean</i>
Tree	<i>down</i>
Configurable	False
Platforms	Supported on all platforms

external *boolean*

Description	Reads true when the IPv6 prefix reachability is external (learned from another protocol).
Context	<i>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-ipv6-reachability ipv6-prefix string external boolean</i>
Tree	<i>external</i>
Configurable	False
Platforms	Supported on all platforms

metric number

Description	The metric to reach this IPv6 prefix.
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
Range	1 to 16777215
Configurable	False
Platforms	Supported on all platforms

mt-id number

Description	A multi-topology ID.
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
Range	0 to 4095
Configurable	False
Platforms	Supported on all platforms

sub-tlvs

Description	SubTLVs of TLV 135, TLV 235, TLV 236 and TLV 237
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> sub-tlvs
Tree	sub-tlvs
Configurable	False
Platforms	Supported on all platforms

route-tag-32bit number

Description	List of 32-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-32bit <i>number</i>
Tree	route-tag-32bit

Range	1 to 4294967295
Configurable	False
Platforms	Supported on all platforms

route-tag-64bit *number*

Description	List of 64-bit administrative tag values associated with the IPv4 prefix.
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> sub-tlvs route-tag-64bit <i>number</i>
Tree	route-tag-64bit
Configurable	False
Platforms	Supported on all platforms

segment-routing-prefix-sid

Description	Carries a segment routing prefix SID
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> sub-tlvs segment-routing-prefix-sid
Tree	segment-routing-prefix-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

algorithm *keyword*

Description	Contains the identifier of the algorithm the router uses to compute the reachability of the prefix to which the Prefix-SID is associated
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> sub-tlvs segment-routing-prefix-sid algorithm <i>keyword</i>
Tree	algorithm
Options	<ul style="list-style-type: none"> • spf • strict-spf
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

explicit-null *boolean*

Description	If set any upstream neighbor of the Prefix-SID originator MUST replace the Prefix-SID with a Prefix-SID that has an Explicit NULL value (0 for IPv4 and 2 for IPv6) before forwarding the packet
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> sub-tlvs segment-routing-prefix-sid explicit-null <i>boolean</i>
Tree	explicit-null
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Prefix-SID has local significance.
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> sub-tlvs segment-routing-prefix-sid local <i>boolean</i>
Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

node-sid *boolean*

Description	If set the prefix SID refers to the router identified by the prefix.
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> sub-tlvs segment-routing-prefix-sid node-sid <i>boolean</i>
Tree	node-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

penultimate-hop-popping *boolean*

Description	If set the penultimate hop MUST NOT pop the Prefix-SID before delivering the packet to the node that advertised the Prefix-SID.
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> sub-tlvs segment-routing-prefix-sid penultimate-hop-popping <i>boolean</i>
Tree	penultimate-hop-popping

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

re-advertised *boolean*

Description	If set the prefix to which this Prefix-SID is attached has been propagated by the router from either another level or from another protocol.
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> sub-tlvs segment-routing-prefix-sid re-advertised <i>boolean</i>
Tree	re-advertised
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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> sub-tlvs segment-routing-prefix-sid sr-index-or-label <i>number</i>
Tree	sr-index-or-label
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Prefix-SID carries a value
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> sub-tlvs segment-routing-prefix-sid value <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

mt-is-reachability [neighbor](#) *string*

Description	Each TLV encodes the identity of an adjacent IS neighbor in a specific topology. TLV type = 222
--------------------	---

Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-is-reachability neighbor string</code>
Tree	<code>mt-is-reachability</code>
Configurable	False
Platforms	Supported on all platforms

neighbor string

Description	An adjacent IS neighbor
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-is-reachability neighbor string</code>
String Length	17
Configurable	False
Platforms	Supported on all platforms

default-metric number

Description	The default metric to reach this adjacent neighbor.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-is-reachability neighbor string default-metric number</code>
Tree	<code>default-metric</code>
Range	1 to 16777215
Configurable	False
Platforms	Supported on all platforms

mt-id number

Description	A multi-topology ID.
Context	<code>network-instance name string protocols isis instance name string level-database level-number number lsp-id string defined-tlvs mt-is-reachability neighbor string mt-id number</code>
Tree	<code>mt-id</code>
Range	0 to 4095
Configurable	False
Platforms	Supported on all platforms

sub-tlvs

Description	SubTLVs of TLV 22 and TLV 222
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> sub-tlvs
Tree	sub-tlvs
Configurable	False
Platforms	Supported on all platforms

ipv4-interface-address *string*

Description	The IPv4 address of the interface to the neighbor. Sub-TLV = 6.
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> sub-tlvs ipv4-interface-address <i>string</i>
Tree	ipv4-interface-address
Configurable	False
Platforms	Supported on all platforms

ipv4-neighbor-address *string*

Description	The IPv4 address of the neighbor. Sub-TLV = 8.
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> sub-tlvs ipv4-neighbor-address <i>string</i>
Tree	ipv4-neighbor-address
Configurable	False
Platforms	Supported on all platforms

ipv6-interface-address *string*

Description	The IPv6 address of the interface to the neighbor. Sub-TLV = 12.
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> sub-tlvs ipv6-interface-address <i>string</i>
Tree	ipv6-interface-address
Configurable	False
Platforms	Supported on all platforms

ipv6-neighbor-address *string*

Description	The IPv4 address of the neighbor. Sub-TLV = 13.
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> sub-tlvs ipv6-neighbor-address <i>string</i>
Tree	ipv6-neighbor-address
Configurable	False
Platforms	Supported on all platforms

link-msd

Description	The maximum segment depth of the link to the neighbor. Sub-TLV = 15.
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> sub-tlvs link-msd
Tree	link-msd
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-info [msd-type](#) (*keyword* | *number*) [msd-value](#) *number*

Description	List of MSD entries
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> sub-tlvs link-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Tree	msd-info
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-type (*keyword* | *number*)

Description	MSD type
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> sub-tlvs link-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Range	2 to 254

Options	• base-mpls-imposition-msd
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-value *number*

Description	A number in the range of 0-255 representing the maximum SID depth; for all MSD-Types, 0 represents the lack of ability to support a SID stack of any depth
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> sub-tlvs link-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

segment-routing-adjacency-sid [sr-index-or-label](#) *number*

Description	List of Adj-SID sub-TLVs associated with the neighbor. Sub-TLV = 31.
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i>
Tree	segment-routing-adjacency-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

adj-set *boolean*

Description	When set, the S-Flag indicates that the Adj-SID refers to a set of adjacencies.
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> adj-set <i>boolean</i>
Tree	adj-set
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

backup *boolean*

Description	If set, the Adj-SID is eligible for protection
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> backup <i>boolean</i>
Tree	backup
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-family *boolean*

Description	If set, then the Adj-SID is used for forwarding IPv6 traffic to the neighbor; else the Adj-SID is used for forwarding IPv4 traffic.
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> ipv6-family <i>boolean</i>
Tree	ipv6-family
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Adj-SID has local significance.
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> local <i>boolean</i>

Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

persistent *boolean*

Description	When set, the P-Flag indicates that the Adj-SID is persistently allocated, i.e., the Adj-SID value remains consistent across router restart and/or interface flap
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> persistent <i>boolean</i>
Tree	persistent
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Adj-SID carries a value
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> value <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

weight *number*

Description	The value represents the weight of the Adj-SID for the purpose of load balancing
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> sub-tlvs segment-routing-adjacency-sid sr-index-or-label <i>number</i> weight <i>number</i>
Tree	weight
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

segment-routing-lan-adjacency-sid sr-index-or-label *number*

Description	List of LAN Adj-SID sub-TLVs. Each describes the set of Adj-SIDs the router assigned to each of its LAN neighbors. Sub-TLV = 32.
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i>
Tree	segment-routing-lan-adjacency-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing an offset in the SID/label space advertised by the router or else a direct encoding of an MPLS label value.
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

adj-set *boolean*

Description	When set, the S-Flag indicates that the Adj-SID refers to a set of adjacencies.
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> adj-set <i>boolean</i>
Tree	adj-set
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

backup *boolean*

Description	If set, the Adj-SID is eligible for protection
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> backup <i>boolean</i>

Tree	backup
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-family *boolean*

Description	If set, then the Adj-SID is used for forwarding IPv6 traffic to the neighbor; else the Adj-SID is used for forwarding IPv4 traffic.
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> ipv6-family <i>boolean</i>
Tree	ipv6-family
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Adj-SID has local significance.
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> local <i>boolean</i>
Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

neighbor-system-id *string*

Description	IS-IS system-ID of the LAN neighbor
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> neighbor-system-id <i>string</i>
Tree	neighbor-system-id
String Length	14
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

persistent *boolean*

Description	When set, the P-Flag indicates that the Adj-SID is persistently allocated, i.e., the Adj-SID value remains consistent across router restart and/or interface flap
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> persistent <i>boolean</i>
Tree	persistent
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

value *boolean*

Description	If set then the Adj-SID carries a value
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> value <i>boolean</i>
Tree	value
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

weight *number*

Description	The value represents the weight of the Adj-SID for the purpose of load balancing
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> sub-tlvs segment-routing-lan-adjacency-sid sr-index-or-label <i>number</i> weight <i>number</i>
Tree	weight
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

multi-topology

Description	The Multi-Topology TLV, type 229.
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
Configurable	False
Platforms	Supported on all platforms

topology *mt-id number*

Description	The list of multi-topology IDs that the router is participating in
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
Configurable	False
Platforms	Supported on all platforms

mt-id *number*

Description	A multi-topology ID.
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>
Range	0 to 4095
Configurable	False
Platforms	Supported on all platforms

attached *boolean*

Description	Reads true when the topology is attached to Level 2
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
Configurable	False
Platforms	Supported on all platforms

overload *boolean*

Description	Reads true when the topology is in overload state.
--------------------	--

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
Configurable	False
Platforms	Supported on all platforms

nlpid *keyword*

Description	Each item represents a network layer protocol supported by the IS-IS Instance.
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
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
Platforms	Supported on all platforms

purge-oi *string*

Description	This indicates System ID that originated a purge.
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
String Length	14
Configurable	False
Platforms	Supported on all platforms

router-capability

Description	Allows a router to announce its capabilities within an IS-IS level or the entire routing domain. TLV = 242.
--------------------	---

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 router-capability
Tree	router-capability
Configurable	False
Platforms	Supported on all platforms

leaked-down *boolean*

Description	When true, the TLV was leaked down from Level 2 to Level 1 and must not be leaked back up to L2
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 router-capability leaked-down <i>boolean</i>
Tree	leaked-down
Configurable	False
Platforms	Supported on all platforms

router-id *string*

Description	Router ID indicating the source of the TLV
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 router-capability router-id <i>string</i>
Tree	router-id
Configurable	False
Platforms	Supported on all platforms

scope-is-domain-wide *boolean*

Description	When true, the TLV MUST be flooded across the entire routing domain. When false, the TLV MUST NOT be leaked between levels.
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 router-capability scope-is-domain-wide <i>boolean</i>
Tree	scope-is-domain-wide
Configurable	False
Platforms	Supported on all platforms

sub-tlvs

Description	Sub-TLVs of TLV 242
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 router-capability sub-tlvs
Tree	sub-tlvs
Configurable	False
Platforms	Supported on all platforms

node-msd

Description	Used to carry the provisioned SID depth of the router originating the capability TLV. Node MSD is the smallest MSD supported by the node on the set of interfaces configured for use by the advertising IGP instance
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 router-capability sub-tlvs node-msd
Tree	node-msd
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-info [msd-type](#) (*keyword* | *number*) [msd-value](#) *number*

Description	List of MSD entries
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 router-capability sub-tlvs node-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Tree	msd-info
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-type (*keyword* | *number*)

Description	MSD type
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 router-capability sub-tlvs node-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Range	2 to 254

Options	• base-mpls-imposition-msd
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

msd-value *number*

Description	A number in the range of 0-255 representing the maximum SID depth; for all MSD-Types, 0 represents the lack of ability to support a SID stack of any depth
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 router-capability sub-tlvs node-msd msd-info msd-type (<i>keyword</i> <i>number</i>) msd-value <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-algorithm

Description	Advertises the IGP algorithms that the router is using
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 router-capability sub-tlvs sr-algorithm
Tree	sr-algorithm
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

algorithm *number*

Description	List of algorithm types supported by the router. Algorithm 0 should always be in the list
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 router-capability sub-tlvs sr-algorithm algorithm <i>number</i>
Tree	algorithm
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-capabilities

Description	Used to advertise its SR data plane capability and the range of MPLS label values each router uses for Segment Routing in the case where global SIDs are allocated.
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 router-capability sub-tlvs sr-capabilities
Tree	sr-capabilities
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-support *boolean*

Description	When true, the router is capable of processing SR-MPLS-encapsulated IPv4 packets on all interfaces
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 router-capability sub-tlvs sr-capabilities ipv4-support <i>boolean</i>
Tree	ipv4-support
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-support *boolean*

Description	When true, the router is capable of processing SR-MPLS-encapsulated IPv6 packets on all interfaces
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 router-capability sub-tlvs sr-capabilities ipv6-support <i>boolean</i>
Tree	ipv6-support
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

srgb-descriptor [sr-index-or-label](#) *number range number*

Description	List of Segment Routing Global Block descriptors
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 router-capability sub-tlvs sr-capabilities srgb-descriptor sr-index-or-label <i>number range number</i>

Tree	srgb-descriptor
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing the first value of the SRGB. The meaning (index or label) is determined from the length of the sub-tlv.
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 router-capability sub-tlvs sr-capabilities srgb-descriptor sr-index-or-label <i>number range number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

range *number*

Description	The number of SRGB elements
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 router-capability sub-tlvs sr-capabilities srgb-descriptor sr-index-or-label <i>number range number</i>
Range	1 to 16777215
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-local-block

Description	Used to advertise the range of labels the node has reserved for local SIDs.
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 router-capability sub-tlvs sr-local-block
Tree	sr-local-block
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

srlb-descriptor [sr-index-or-label](#) *number range number*

Description	List of Segment Routing Local Block descriptors
--------------------	---

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 router-capability sub-tlvs sr-local-block srlb-descriptor sr-index-or-label <i>number range number</i>
Tree	srlb-descriptor
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sr-index-or-label *number*

Description	An index representing the first value of the SRLB. The meaning (index or label) is determined from the length of the sub-tlv.
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 router-capability sub-tlvs sr-local-block srlb-descriptor sr-index-or-label <i>number range number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

range *number*

Description	The number of SRLB elements
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 router-capability sub-tlvs sr-local-block srlb-descriptor sr-index-or-label <i>number range number</i>
Range	1 to 16777215
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

te-router-id *string*

Description	A single stable address that can always be referenced in a path that will be reachable from multiple hops away. TLV = 134.
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 te-router-id <i>string</i>
Tree	te-router-id
Configurable	False
Platforms	Supported on all platforms

maximum-area-addresses *number*

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.
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
Configurable	False
Platforms	Supported on all platforms

pdu-length *number*

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.
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
Configurable	False
Platforms	Supported on all platforms

pdu-type *number*

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.
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
Configurable	False
Platforms	Supported on all platforms

pkt-version *number*

Description	The value indicates the version of the ISIS protocol that has generated the Packet.
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
Configurable	False

Platforms Supported on all platforms

remaining-lifetime *number*

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.

Context [network-instance name string protocols isis instance name string level-database level-number number lsp-id string remaining-lifetime number](#)

Tree [remaining-lifetime](#)

Range 0 to 65535

Units seconds

Configurable False

Platforms Supported on all platforms

sequence-number *string*

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.

Context [network-instance name string protocols isis instance name string level-database level-number number lsp-id string sequence-number string](#)

Tree [sequence-number](#)

Configurable False

Platforms Supported on all platforms

system-id-len *number*

Description The value indicates the length of the system-id as used by the originator.

Context [network-instance name string protocols isis instance name string level-database level-number number lsp-id string system-id-len number](#)

Tree [system-id-len](#)

Configurable False

Platforms Supported on all platforms

undefined-tlvs *string*

Description	Undefined TLV-s as contents of the LSP.
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
String Length	27 to 9190
Configurable	False
Platforms	Supported on all platforms

version *number*

Description	The value indicates the version of the ISIS protocol that has generated the LSP
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
Configurable	False
Platforms	Supported on all platforms

max-ecmp-paths *number*

Description	The maximum number of ECMP next-hops to program into the FIB for every IP prefix
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> max-ecmp-paths <i>number</i>
Tree	max-ecmp-paths
Range	1 to 64
Default	1
Configurable	True
Platforms	Supported on all platforms

net *string*

Description	ISIS network entity title (NET)
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> net <i>string</i>
Tree	net
Configurable	True
Platforms	Supported on all platforms

Max. Elements 1

oper-area-id *string*

Description The list of area IDs associated with this IS router

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [oper-area-id](#) *string*

Tree [oper-area-id](#)

String Length 2 to 38

Configurable False

Platforms Supported on all platforms

oper-state *keyword*

Description The value of the this object indicates the operational state of the destination.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [oper-state](#) *keyword*

Tree [oper-state](#)

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
- low-power

	Component is offline due to insufficient system power
• degraded	Component or process is in a degraded state
• warm-reboot	Component or process is currently warm rebooting
	Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
• waiting	Component or process is currently waiting
	Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

oper-system-id *string*

Description	The ID for this instance of the Integrated IS-IS protocol.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> oper-system-id <i>string</i>
Tree	oper-system-id
String Length	14
Configurable	False
Platforms	Supported on all platforms

overload

Description	Specifies isis routing instance behavior regarding overload
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload
Tree	overload
Configurable	True
Platforms	Supported on all platforms

advertise-external *boolean*

Description	When set to true, external (non-ISIS) routes continue to be advertised when the router is in overload.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload advertise-external <i>boolean</i>
Tree	advertise-external
Default	false
Configurable	True
Platforms	Supported on all platforms

advertise-interlevel *boolean*

Description	When set to true, L1->L2 and L2->L1 inter-level routes continue to be advertised when the router is in overload.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload advertise-interlevel <i>boolean</i>
Tree	advertise-interlevel
Default	false
Configurable	True
Platforms	Supported on all platforms

immediate

Description	Options for advertising an overloaded state immediately
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload immediate
Tree	immediate
Configurable	True
Platforms	Supported on all platforms

max-metric *boolean*

Description	When set to true transit links are advertised with a wide metric of 0xfffffe and a narrow metric of 0x3f
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload immediate max-metric <i>boolean</i>
Tree	max-metric
Default	false

Configurable	True
Platforms	Supported on all platforms

set-bit *boolean*

Description	When set to true, the Overload bit is set
Context	network-instance name string protocols isis instance name string overload immediate set-bit boolean
Tree	set-bit
Default	false
Configurable	True
Platforms	Supported on all platforms

instance-is-in-overload *boolean*

Description	When set to true the IS-IS instance is currently in overload state.
Context	network-instance name string protocols isis instance name string overload instance-is-in-overload boolean
Tree	instance-is-in-overload
Configurable	False
Platforms	Supported on all platforms

on-boot

Description	Options for advertising an overloaded state whenever the IS-IS process restarts
Context	network-instance name string protocols isis instance name string overload on-boot
Tree	on-boot
Configurable	True
Platforms	Supported on all platforms

max-metric *boolean*

Description	When set to true transit links are advertised with a wide metric of 0xfffffe and a narrow metric of 0x3f
Context	network-instance name string protocols isis instance name string overload on-boot max-metric boolean

Tree	max-metric
Configurable	True
Platforms	Supported on all platforms

set-bit *boolean*

Description	When set to true, the Overload bit is set
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
Configurable	True
Platforms	Supported on all platforms

timeout *number*

Description	Specifies the time that the router should remain in overload state after the IS-IS process restarts
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> overload on-boot timeout <i>number</i>
Tree	timeout
Range	60 to 1800
Units	seconds
Configurable	True
Platforms	Supported on all platforms

poi-tlv *boolean*

Description	When set to true, a TLV is added to purge to record the system ID of the IS generating the purge.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> poi-tlv <i>boolean</i>
Tree	poi-tlv
Default	false
Configurable	True
Platforms	Supported on all platforms

restarting-neighbor-list

Description	The list of neighbors that have restarted recently and that are currently being helped.
Context	network-instance name string protocols isis instance name string restarting-neighbor-list
Tree	restarting-neighbor-list
Configurable	False
Platforms	Supported on all platforms

neighbor [system-id string](#)

Description	The list of neighbors that have restarted recently and that are currently being helped.
Context	network-instance name string protocols isis instance name string restarting-neighbor-list neighbor system-id string
Tree	neighbor
Configurable	False
Platforms	Supported on all platforms

system-id [string](#)

Description	The neighbor router's system ID.
Context	network-instance name string protocols isis instance name string restarting-neighbor-list neighbor system-id string
String Length	14
Configurable	False
Platforms	Supported on all platforms

hostname [string](#)

Description	The hostname of the neighbor, as learned by TLV 137.
Context	network-instance name string protocols isis instance name string restarting-neighbor-list neighbor system-id string hostname string
Tree	hostname
Configurable	False
Platforms	Supported on all platforms

segment-routing

Description	Enter the segment-routing context
Context	network-instance name string protocols isis instance name string segment-routing
Tree	segment-routing
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

mpls

Description	Context used to configure SR-MPLS options
Context	network-instance name string protocols isis instance name string segment-routing mpls
Tree	mpls
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

sid-database

Description	Database of all prefix SIDs associated with the IS-IS instance.
Context	network-instance name string protocols isis instance name string segment-routing mpls sid-database
Tree	sid-database
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

prefix-sid [prefix \(ipv4-prefix | ipv6-prefix\)](#) [sid-label-value number multi-topology-id number algorithm number](#)

Description	List of prefix SIDs
Context	network-instance name string protocols isis instance name string segment-routing mpls sid-database prefix-sid prefix (ipv4-prefix ipv6-prefix) sid-label-value number multi-topology-id number algorithm number
Tree	prefix-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

prefix (*ipv4-prefix | ipv6-prefix*)

Description	The IPv4 or IPv6 prefix associated with the SID.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sid-label-value *number*

Description	The MPLS label value associated with the SID.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i>
Range	16 to 1048575
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

multi-topology-id *number*

Description	The multi-topology ID that provided the prefix SID
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i>
Range	0 to 4095
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

algorithm *number*

Description	Contains the identifier of the algorithm the router uses to compute the reachability of the prefix to which the Prefix-SID is associated
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

active *boolean*

Description	When false, the prefix SID is inactive. It could be inactive for any of these reasons:
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> active <i>boolean</i>
Tree	active
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

prefix-conflict *boolean*

Description	Reads true when the prefix SID entry is involved in a prefix conflict within the scope of this IS-IS instance. This occurs when there are multiple entries for the same (prefix, multi-topology-id, algorithm). All the conflicting entries become inactive except for the one with the smallest sid-index.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> prefix-conflict <i>boolean</i>
Tree	prefix-conflict
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sid-conflict *boolean*

Description	Reads true when the prefix SID entry is involved in a SID conflict within the scope of this IS-IS instance. This occurs when the same SID has been assigned to different prefixes after first eliminating entries that have lost the prefix-conflict comparison. All entries involved in a SID conflict that do not have the absolute lowest 'preference' value become inactive. In the SRL implementation SID entries associated with interfaces of this IS-IS instance are considered to have a lower numerical preference than remote prefix-sid entries. If there are still SID conflicts then all the remaining conflicting entries become inactive except for the one with the smallest sid-index.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> sid-conflict <i>boolean</i>
Tree	sid-conflict
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sid-out-of-range *boolean*

Description	Reads true when a received prefix SID from another router has a SID index or label value that is not within the locally defined SRGB range of the network instance; the prefix SID entry will be inactive.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> sid-out-of-range <i>boolean</i>
Tree	sid-out-of-range
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

source-router [system-id](#) *string* [level-number](#) *number*

Description	The ISIS routers that provided the prefix SID. (Multiple in the case of redistribution.)
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i>
Tree	source-router
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

system-id *string*

Description	The system-id of an ISIS router that originated or redistributed the prefix SID
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i>
String Length	14
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

level-number *number*

Description	The level of the LSP that advertises the prefix SID
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-

	value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i>
Range	1 to 2
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

flags

Description	Flags that characterize the prefix SID
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> flags
Tree	flags
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

explicit-null *boolean*

Description	If set any upstream neighbor of the Prefix-SID originator MUST replace the Prefix-SID with a Prefix-SID that has an Explicit NULL value (0 for IPv4 and 2 for IPv6) before forwarding the packet
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> flags explicit-null <i>boolean</i>
Tree	explicit-null
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local *boolean*

Description	If set, then the value/index carried by the Prefix-SID has local significance.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> flags local <i>boolean</i>
Tree	local
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

node-sid *boolean*

Description	If set the prefix SID refers to the router identified by the prefix.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> flags node-sid <i>boolean</i>
Tree	node-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

penultimate-hop-popping *boolean*

Description	If set the penultimate hop MUST NOT pop the Prefix-SID before delivering the packet to the node that advertised the Prefix-SID.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> flags penultimate-hop-popping <i>boolean</i>
Tree	penultimate-hop-popping
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

re-advertised *boolean*

Description	If set the prefix to which this Prefix-SID is attached was propagated from another level or from another protocol.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> flags re-advertised <i>boolean</i>
Tree	re-advertised
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local-system *boolean*

Description	True when the system ID belongs to the local system.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-

	value <i>number</i> multi-topology-id <i>number</i> algorithm <i>number</i> source-router system-id <i>string</i> level-number <i>number</i> local-system <i>boolean</i>
Tree	local-system
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Instance level statistics
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

last-partial-spf *string*

Description	The elapsed time since the last time a partial SPF run was run on either the L1 or L2 LSDB
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
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-spf *string*

Description	The elapsed time since the last time a full SPF run was run on either the L1 or L2 LSDB
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics last-spf <i>string</i>
Tree	last-spf
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

partial-spf-runs *number*

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
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
Default	0
Configurable	False
Platforms	Supported on all platforms

pdu [pdu-name](#) *keyword*

Description	List of PDUs processed by the IS-IS instance since the IS-IS manager restarted
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i>
Tree	pdu
Configurable	False
Platforms	Supported on all platforms

pdu-name *keyword*

Description	The PDU type that was processed
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i>
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
Platforms	Supported on all platforms

dropped *number*

Description	The number of PDUs that were received and dropped
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i> dropped <i>number</i>
Tree	dropped
Default	0
Configurable	False
Platforms	Supported on all platforms

processed *number*

Description	The number of PDUs that were received and processed
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i> processed <i>number</i>
Tree	processed
Default	0
Configurable	False
Platforms	Supported on all platforms

received *number*

Description	The number of PDUs that were received
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics pdu pdu-name <i>keyword</i> received <i>number</i>
Tree	received
Default	0
Configurable	False
Platforms	Supported on all platforms

sent *number*

Description	The number of PDUs that were transmitted
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
Default	0

Configurable	False
Platforms	Supported on all platforms

spf-runs *number*

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
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics spf-runs <i>number</i>
Tree	spf-runs
Default	0
Configurable	False
Platforms	Supported on all platforms

timers

Description	Container for IS-IS timers applicable at the instance level
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers
Tree	timers
Configurable	True
Platforms	Supported on all platforms

lsp-generation

Description	Container with options for specifying LSP generation timer values
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers lsp-generation
Tree	lsp-generation
Configurable	True
Platforms	Supported on all platforms

initial-wait *number*

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
--------------------	---

Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers lsp-generation initial-wait <i>number</i>
Tree	initial-wait
Range	10 to 100000
Default	10
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

max-wait *number*

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
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
Range	10 to 120000
Default	5000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

second-wait *number*

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
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
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True

Platforms Supported on all platforms

Isp-lifetime *number*

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.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [timers lsp-lifetime](#) *number*

Tree [Isp-lifetime](#)

Range 350 to 65535

Default 1200

Units seconds

Configurable True

Platforms Supported on all platforms

Isp-refresh

Description Configure LSP refresh timers.

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [timers lsp-refresh](#)

Tree [Isp-refresh](#)

Configurable True

Platforms Supported on all platforms

half-lifetime *boolean*

Description When set to true, the LSP refresh interval is half the Isp-lifetime

Context [network-instance name](#) *string* [protocols isis instance name](#) *string* [timers lsp-refresh half-lifetime](#) *boolean*

Tree [half-lifetime](#)

Default true

Configurable True

Platforms Supported on all platforms

interval *number*

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.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers lsp-refresh interval <i>number</i>
Tree	interval
Range	150 to 65535
Default	600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

spf

Description	Container with options for specifying SPF timer values
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers spf
Tree	spf
Configurable	True
Platforms	Supported on all platforms

initial-wait *number*

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
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> timers spf initial-wait <i>number</i>
Tree	initial-wait
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

max-wait number

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
Context	network-instance name string protocols isis instance name string timers spf max-wait number
Tree	max-wait
Range	10 to 120000
Default	10000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

second-wait number

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
Context	network-instance name string protocols isis instance name string timers spf second-wait number
Tree	second-wait
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

trace-options

Description	Instance level debug trace options for IS-IS
Context	network-instance name string protocols isis instance name string trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace keyword

Description	List of tracing options
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> trace-options trace keyword
Tree	trace
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
Platforms	Supported on all platforms

transport

Description	Enter the transport context
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> transport
Tree	transport
Configurable	True
Platforms	Supported on all platforms

lsp-mtu-size number

Description	Sets the maximum size of LSPs generated by this router
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> transport lsp-mtu-size number

Tree	lsp-mtu-size
Range	490 to 9490
Default	1492
Units	bytes
Configurable	True
Platforms	Supported on all platforms

ldp

Description	Container for LDP configuration and state.
Context	network-instance name <i>string</i> protocols ldp
Tree	ldp
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

admin-state *keyword*

Description	Administratively enable or disable LDP.
Context	network-instance name <i>string</i> protocols ldp admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

discovery

Description	Neighbor discovery configuration and operational state.
Context	network-instance name <i>string</i> protocols ldp discovery
Tree	discovery
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

interfaces

Description	The complete set of interfaces used for LDP Basic Discovery.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces
Tree	interfaces
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hello-holdtime *number*

Description	The time interval for which a LDP link Hello adjacency is maintained in the absence of link Hello messages from the LDP neighbor
Context	network-instance name <i>string</i> protocols ldp discovery interfaces hello-holdtime <i>number</i>
Tree	hello-holdtime
Range	15 to 3600
Default	15
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hello-interval *number*

Description	The interval between consecutive LDP link Hello messages used in basic LDP discovery
Context	network-instance name <i>string</i> protocols ldp discovery interfaces hello-interval <i>number</i>
Tree	hello-interval
Range	5 to 1200
Default	5
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

interface [name](#) *reference*

Description	List of LDP interfaces used for LDP Basic Discovery.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i>

Tree	interface
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name reference

Description	Reference to a specific subinterface that is bound to the network instance
Context	network-instance name string protocols ldp discovery interfaces interface name reference
Reference	network-instance name string interface name string
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hello-holdtime number

Description	The time interval for which a LDP link Hello adjacency is maintained in the absence of link Hello messages from the LDP neighbor
Context	network-instance name string protocols ldp discovery interfaces interface name reference hello-holdtime number
Tree	hello-holdtime
Range	15 to 3600
Default	15
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hello-interval number

Description	The interval between consecutive LDP link Hello messages used in basic LDP discovery
Context	network-instance name string protocols ldp discovery interfaces interface name reference hello-interval number
Tree	hello-interval
Range	5 to 1200
Default	5
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv4

Description	Enter the ipv4 context
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4
Tree	ipv4
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

admin-state *keyword*

Description	Administratively enable or disable LDP discovery for IPv4 on a particular interface.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hello-adjacencies

Description	Container with a list of hello adjacencies.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies
Tree	hello-adjacencies
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

adjacency *lsr-id* *reference* *label-space-id* *reference*

Description	List of hello adjacencies.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency <i>lsr-id</i> <i>reference</i> label-space-id <i>reference</i>
Tree	adjacency

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

lsr-id reference

Description	The LSR ID of the peer, as a portion of the peer LDP ID.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id reference label-space-id reference
Reference	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-space-id reference

Description	The Label Space ID of the peer, as a portion of the peer LDP ID.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id reference label-space-id reference
Reference	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

hello-holdtime

Description	Container for hello holdtime state information.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id reference label-space-id reference hello-holdtime
Tree	hello-holdtime
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

negotiated number

Description	The holdtime negotiated between this LSR and the adjacent LSR.
--------------------	--

Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id <i>reference</i> label-space-id <i>reference</i> hello-holdtime negotiated <i>number</i>
Tree	negotiated
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

neighbor-proposed *number*

Description	The holdtime value learned from the adjacent LSR.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id <i>reference</i> label-space-id <i>reference</i> hello-holdtime neighbor-proposed <i>number</i>
Tree	neighbor-proposed
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

remaining *number*

Description	The time remaining until the holdtime timer expires.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id <i>reference</i> label-space-id <i>reference</i> hello-holdtime remaining <i>number</i>
Tree	remaining
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

hello-received *number*

Description	The number of Hello messages received.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 hello-adjacencies adjacency lsr-id <i>reference</i> label-space-id <i>reference</i> hello-received <i>number</i>
Tree	hello-received
Default	0
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

hello-sent *number*

Description The number of Hello messages sent.

Context [network-instance name](#) *string* [protocols ldp discovery interfaces interface name](#) *reference* [ipv4 hello-adjacencies adjacency lsr-id](#) *reference* [label-space-id](#) *reference* [hello-sent](#) *number*

Tree [hello-sent](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

local-address *string*

Description Local address of the hello adjacency.

Context [network-instance name](#) *string* [protocols ldp discovery interfaces interface name](#) *reference* [ipv4 hello-adjacencies adjacency lsr-id](#) *reference* [label-space-id](#) *reference* [local-address](#) *string*

Tree [local-address](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

remote-address *string*

Description Remote address of the hello adjacency.

Context [network-instance name](#) *string* [protocols ldp discovery interfaces interface name](#) *reference* [ipv4 hello-adjacencies adjacency lsr-id](#) *reference* [label-space-id](#) *reference* [remote-address](#) *string*

Tree [remote-address](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

last-oper-state-change *string*

Description The last time when the IPv4 oper-state changed.

Context [network-instance name](#) *string* [protocols ldp discovery interfaces interface name](#) *reference* [ipv4 last-oper-state-change](#) *string*

Tree [last-oper-state-change](#)

String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

oper-down-reason *keyword*

Description	Reason for the LDP interface being down from an IPv4 perspective.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • ldp-interface-admin-down • ldp-instance-oper-down • network-instance-subinterface-down • out-of-resources • unknown
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

oper-state *keyword*

Description	Operational state of IPv4 on the LDP interface
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up • down
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Statistics objects.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics
Tree	statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

hello-message-errors

Description	Counters for received Hello message errors
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-message-errors
Tree	hello-message-errors
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-message-length *number*

Description	The number of Hello messages received with a bad message length
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-message-errors bad-message-length number
Tree	bad-message-length
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-pdu-length *number*

Description	The number of Hello messages received with a bad PDU length
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-message-errors bad-pdu-length number
Tree	bad-pdu-length
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-protocol-version *number*

Description	The number of Hello messages received with a bad protocol version
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-message-errors bad-protocol-version number
Tree	bad-protocol-version
Default	0

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

malformed-tlv-value *number*

Description	The number of Hello messages received with a malformed TLV value
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-message-errors malformed-tlv-value number
Tree	malformed-tlv-value
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

hello-received *number*

Description	The number of Hello messages received.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-received number
Tree	hello-received
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

hello-sent *number*

Description	The number of Hello messages sent.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 statistics hello-sent number
Tree	hello-sent
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

trace-options

Description	Configure event/packet tracing for one specific LDP interface.
--------------------	--

Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 trace-options
Tree	trace-options
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

trace keyword

Description	Specifies the trace information to be captured.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>reference</i> ipv4 trace-options trace keyword
Tree	trace
Options	<ul style="list-style-type: none"> • all Trace all events and packets • events-discovery Trace session related events • messages-hello Trace Hello packets • messages-hello-detail Trace LDP Hello packets with detailed output
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

trace-options

Description	Configure event/packet tracing for all LDP interfaces.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces trace-options
Tree	trace-options
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

trace keyword

Description	Specifies the trace information to be captured.
Context	network-instance name <i>string</i> protocols ldp discovery interfaces trace-options trace keyword
Tree	trace

Options	<ul style="list-style-type: none"> • all Trace all events and packets • events-discovery Trace session related events • messages-hello Trace Hello packets • messages-hello-detail Trace LDP Hello packets with detailed output
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

graceful-restart

Description	Attributes for graceful restart.
Context	network-instance name <i>string</i> protocols ldp graceful-restart
Tree	graceful-restart
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

helper-enable *boolean*

Description	Enable or disable graceful restart as a helper.
Context	network-instance name <i>string</i> protocols ldp graceful-restart helper-enable <i>boolean</i>
Tree	helper-enable
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

max-reconnect-time *number*

Description	Specifies the maximum time interval, in seconds, that this router is willing to wait for the remote LDP peer to reconnect after an LDP communication failure.
Context	network-instance name <i>string</i> protocols ldp graceful-restart max-reconnect-time <i>number</i>
Tree	max-reconnect-time
Range	10 to 1800

Default	120
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

max-recovery-time *number*

Description	Specifies the maximum time interval, in seconds, that this router is willing to preserve its MPLS forwarding state after receiving the Initialization message from the restarted LDP peer.
Context	network-instance name <i>string</i> protocols ldp graceful-restart max-recovery-time <i>number</i>
Tree	max-recovery-time
Range	30 to 3600
Default	120
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv4

Description	Container for configuration and state related to the IPv4 address family.
Context	network-instance name <i>string</i> protocols ldp ipv4
Tree	ipv4
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

bindings

Description	LDP address and label binding information.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings
Tree	bindings
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

advertised-address

Description	Enter the advertised-address context
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-address
Tree	advertised-address
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer [lsr-id reference](#) [label-space-id reference](#)

Description	List of LDP peers towards which IPv4 address bindings have been sent.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-address peer lsr-id reference label-space-id reference
Tree	peer
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

lsr-id reference

Description	The LSR ID of the peer, as a portion of the peer LDP ID.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-address peer lsr-id reference label-space-id reference
Reference	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-space-id reference

Description	The Label Space ID of the peer, as a portion of the peer LDP ID.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-address peer lsr-id reference label-space-id reference
Reference	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ip-address *string*

Description	The list of IPv4 address bindings sent to the peer
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-address peer lsr-id <i>reference</i> label-space-id <i>reference</i> ip-address <i>string</i>
Tree	ip-address
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

advertised-prefix-fecs [fec](#) *string* [lsr-id](#) *reference* [label-space-id](#) *reference*

Description	List of IPv4 FEC-label bindings advertised to LDP peers.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i>
Tree	advertised-prefix-fecs
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fec *string*

Description	The prefix FEC value in the FEC-label binding, advertised in a Label Mapping message sent to a peer.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

lsr-id *reference*

Description	The LSR ID of the peer, as a portion of the peer LDP ID.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i>
Reference	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-space-id *reference*

Description	The Label Space ID of the peer, as a portion of the peer LDP ID.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id reference label-space-id reference
Reference	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

egress-lsr-fec *boolean*

Description	When set true, the router is the egress LSR for the FEC (the FEC is locally originated).
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id reference label-space-id reference egress-lsr-fec <i>boolean</i>
Tree	egress-lsr-fec
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label (*number* | *keyword*)

Description	Advertised label value.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id reference label-space-id reference label (<i>number</i> <i>keyword</i>)
Tree	label
Range	16 to 1048575
Options	<ul style="list-style-type: none"> • IPV4_EXPLICIT_NULL • IPV6_EXPLICIT_NULL • IMPLICIT_NULL
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-status *keyword*

Description	Enter the label-status context
--------------------	--------------------------------

Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i> label-status <i>keyword</i>
Tree	label-status
Options	<ul style="list-style-type: none"> released withdrawn withdraw-pending
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-type *keyword*

Description	The label type of the advertised label.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings advertised-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i> label-type <i>keyword</i>
Tree	label-type
Options	<ul style="list-style-type: none"> pop An advertised label that is programmed with a POP operation. swap An advertised label that is programmed with a SWAP operation.
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

received-address

Description	Enter the received-address context
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings received-address
Tree	received-address
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer [lsr-id](#) *reference* [label-space-id](#) *reference*

Description	List of LDP peers from which IPv4 address bindings have been received.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings received-address peer lsr-id <i>reference</i> label-space-id <i>reference</i>
Tree	peer
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

lsr-id reference

Description The LSR ID of the peer, as a portion of the peer LDP ID.

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-address](#) [peer lsr-id reference](#) [label-space-id reference](#)

Reference [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number*

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

label-space-id reference

Description The Label Space ID of the peer, as a portion of the peer LDP ID.

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-address](#) [peer lsr-id reference](#) [label-space-id reference](#)

Reference [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number*

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

ip-address string

Description The list of IPv4 address bindings received from the peer

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-address](#) [peer lsr-id reference](#) [label-space-id reference](#) [ip-address](#) *string*

Tree [ip-address](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

received-prefix-fecs [fec](#) *string* [lsr-id reference](#) [label-space-id reference](#)

Description List of IPv4 FEC-label bindings received from LDP peers.

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-prefix-fecs](#) [fec](#) *string* [lsr-id reference](#) [label-space-id reference](#)

Tree [received-prefix-fecs](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

fec string

Description The prefix FEC value in the FEC-label binding, learned in a Label Mapping message received from a peer.

Context [network-instance name string protocols ldp ipv4 bindings received-prefix-fecs fec string lsr-id reference label-space-id reference](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

lsr-id reference

Description The LSR ID of the peer, as a portion of the peer LDP ID.

Context [network-instance name string protocols ldp ipv4 bindings received-prefix-fecs fec string lsr-id reference label-space-id reference](#)

Reference [network-instance name string protocols ldp peers peer lsr-id string label-space-id number](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

label-space-id reference

Description The Label Space ID of the peer, as a portion of the peer LDP ID.

Context [network-instance name string protocols ldp ipv4 bindings received-prefix-fecs fec string lsr-id reference label-space-id reference](#)

Reference [network-instance name string protocols ldp peers peer lsr-id string label-space-id number](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

ingress-lsr-fec boolean

Description When set true, the router is an ingress LSR for the FEC.

Context [network-instance name string protocols ldp ipv4 bindings received-prefix-fecs fec string lsr-id reference label-space-id reference ingress-lsr-fec boolean](#)

Tree [ingress-lsr-fec](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

label (*number* | *keyword*)

Description Received label value.

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-prefix-fecs fec](#) *string* [lsr-id reference](#) [label-space-id reference](#) [label \(number | keyword\)](#)

Tree [label](#)

Range 16 to 1048575

Options

- IPV4_EXPLICIT_NULL
- IPV6_EXPLICIT_NULL
- IMPLICIT_NULL

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

next-hop [index number](#)

Description List of ECMP next-hops towards the LDP peer

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-prefix-fecs fec](#) *string* [lsr-id reference](#) [label-space-id reference](#) [next-hop index number](#)

Tree [next-hop](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

index *number*

Description Label ID index entry

Context [network-instance name](#) *string* [protocols ldp ipv4 bindings received-prefix-fecs fec](#) *string* [lsr-id reference](#) [label-space-id reference](#) [next-hop index number](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

interface *string*

Description The outgoing interface towards the LDP peer

Context	network-instance name <i>string</i> protocols ldp ipv4 bindings received-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i> next-hop index number interface <i>string</i>
Tree	interface
String Length	5 to 25
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

next-hop (*ipv4-address* | *ipv6-address*)

Description	The IP next-hop towards the LDP peer
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings received-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i> next-hop index number next-hop (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	next-hop
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

not-used-reason *keyword*

Description	The reason why the label mapping is not being used in the dataplane.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings received-prefix-fecs fec <i>string</i> lsr-id <i>reference</i> label-space-id <i>reference</i> not-used-reason keyword
Tree	not-used-reason
Options	<ul style="list-style-type: none"> • non-ipv4-host-fec The received FEC is not a /32 IPv4 FEC prefix. • exceeds-multipath-limit The LDP multipath ECMP limit has been reached • exceeds-fec-limit The FEC limit has been reached • fec-unresolved The IP prefix FEC is unused because there is no resolving route matching the IP prefix
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used-in-forwarding *boolean*

Description	Reads true if the label is used in forwarding and has been programmed for a push operation.
Context	network-instance name <i>string</i> protocols ldp ipv4 bindings received-prefix-fecs fec <i>string</i> lsr-id reference label-space-id reference used-in-forwarding <i>boolean</i>
Tree	used-in-forwarding
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fec-resolution

Description	Container with options for controlling IPv4 prefix FEC resolution
Context	network-instance name <i>string</i> protocols ldp ipv4 fec-resolution
Tree	fec-resolution
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

longest-prefix *boolean*

Description	<p>When this is set to true IPv4 prefix FECs can be resolved by less-specific IPv4 routes in the route table, as long as the prefix bits of the route match the prefix bits of the FEC; the IP route with the longest prefix match is the route that is used to resolve the FEC.</p> <p>When this is set to false, IPv4 prefix FECs can only be resolved by routes that are an exact match of the FEC in terms of prefix length.</p>
Context	network-instance name <i>string</i> protocols ldp ipv4 fec-resolution longest-prefix <i>boolean</i>
Tree	longest-prefix
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

last-oper-state-change *string*

Description	The last time that the IPv4 oper-state changed.
Context	network-instance name <i>string</i> protocols ldp ipv4 last-oper-state-change <i>string</i>
Tree	last-oper-state-change

String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

oper-down-reason *keyword*

Description	The reason for the LDP for IPv4 being operationally down
Context	network-instance name <i>string</i> protocols ldp ipv4 oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • ldp-admin-disabled • mpls-admin-disabled • no-system-ipv4-address System IPv4 address is used as the LSR ID. If this dependency is missing LDP is down. • net-instance-mgr-down • label-block-unavailable • no-resource Memory allocation failure • unknown Other failure reason
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

oper-state *keyword*

Description	The operational state of LDP for IPv4
Context	network-instance name <i>string</i> protocols ldp ipv4 oper-state <i>keyword</i>
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

oper-up-to-down-transitions *number*

Description	The number of times the oper state for IPv4 has transitioned from up to down
Context	network-instance name <i>string</i> protocols ldp ipv4 oper-up-to-down-transitions <i>number</i>
Tree	oper-up-to-down-transitions
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

lsr-id *string*

Description	Returns the value that is being used as the LDP LSR ID. Currently, this is always the router ID of the default network-instance.
Context	network-instance name <i>string</i> protocols ldp lsr-id <i>string</i>
Tree	lsr-id
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

multipath

Description	Container with options to configure load-balancing over equal-cost paths
Context	network-instance name <i>string</i> protocols ldp multipath
Tree	multipath
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

max-paths *number*

Description	Specifies the maximum number of next-hops used for load-balancing toward towards a given FEC
Context	network-instance name <i>string</i> protocols ldp multipath max-paths <i>number</i>
Tree	max-paths
Range	1 to 64
Default	1
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

peers

Description	Configuration and state related to peers
Context	network-instance name <i>string</i> protocols ldp peers
Tree	peers
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

peer *lsr-id string label-space-id number*

Description	List of peers.
Context	network-instance name string protocols ldp peers peer lsr-id string label-space-id number
Tree	peer
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

lsr-id *string*

Description	The LSR ID of the peer, to identify the globally unique LSR. This is the first four octets of the LDP ID. This leaf is used together with the leaf 'label-space-id' to form the LDP ID.
Context	network-instance name string protocols ldp peers peer lsr-id string label-space-id number
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

label-space-id *number*

Description	The Label Space ID of the peer, to identify a specific label space within the LSR. This is the last two octets of the LDP ID. This leaf is used together with the leaf 'lsr-id' to form the LDP ID.
Context	network-instance name string protocols ldp peers peer lsr-id string label-space-id number
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

end-of-lib

Description	Container with state information pertaining to sent and received End of LIB markers.
Context	network-instance name string protocols ldp peers peer lsr-id string label-space-id number end-of-lib
Tree	end-of-lib
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-prefix-fecs

Description	Enter the ipv4-prefix-fecs context
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> end-of-lib ipv4-prefix-fecs
Tree	ipv4-prefix-fecs
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

received *boolean*

Description	When this is true, an End-of-LIB marker was received from the LDP peer
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> end-of-lib ipv4-prefix-fecs received <i>boolean</i>
Tree	received
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sent *boolean*

Description	When this is true, an End-of-LIB marker was sent to the LDP peer
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> end-of-lib ipv4-prefix-fecs sent <i>boolean</i>
Tree	sent
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fec-limit *number*

Description	The maximum number of FECs of all types combined that will be accepted from the peer. The value 0 implies no limit.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> fec-limit <i>number</i>
Tree	fec-limit
Default	0
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

fec-limit-exceeded *boolean*

Description	Reads true when the peer has sent more FECs than the configured limit.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> fec-limit-exceeded <i>boolean</i>
Tree	fec-limit-exceeded
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

graceful-restart

Description	Graceful restart operational state.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> graceful-restart
Tree	graceful-restart
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer-reconnect-time *number*

Description	The requested reconnect time.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> graceful-restart peer-reconnect-time <i>number</i>
Tree	peer-reconnect-time
Range	10 to 1800
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer-recovery-time *number*

Description	The requested recovery time.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> graceful-restart peer-recovery-time <i>number</i>
Tree	peer-recovery-time
Range	30 to 3600
Default	120

Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer-restarting *boolean*

Description	If true, the peer is currently in the process of restarting
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> graceful-restart peer-restarting <i>boolean</i>
Tree	peer-restarting
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-advertisement-mode

Description	Label advertisement mode state.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> label-advertisement-mode
Tree	label-advertisement-mode
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

negotiated *keyword*

Description	Negotiated Label Advertisement Mode.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> label-advertisement-mode negotiated <i>keyword</i>
Tree	negotiated
Options	<ul style="list-style-type: none"> • downstream-unsolicited Downstream Unsolicited • downstream-on-demand Downstream on Demand
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-oper-state-change *string*

Description	Last time the peer state changed.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> last-oper-state-change <i>string</i>
Tree	last-oper-state-change
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

overload

Description	Overload state of the session
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> overload
Tree	overload
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

local-router-is-overloaded *boolean*

Description	This router transmitted an overload TLV requesting that the peer stop advertising new FECs
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> overload local-router-is-overloaded <i>boolean</i>
Tree	local-router-is-overloaded
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer-is-overloaded *boolean*

Description	The peer has sent an overload TLV to this router requesting that we stop advertising new FECs
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> overload peer-is-overloaded <i>boolean</i>
Tree	peer-is-overloaded
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

received-capabilities

Description	Capabilities signalled by the peer
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities
Tree	received-capabilities
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

dual-stack-capability *boolean*

Description	Dual stack capability. TLV 0x0701
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities dual-stack-capability <i>boolean</i>
Tree	dual-stack-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

dynamic-capability *boolean*

Description	Dynamic capability advertisement capability. Indicates support for Capability messages. TLV 0x0506
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities dynamic-capability <i>boolean</i>
Tree	dynamic-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

entropy-label-capability *boolean*

Description	Entropy label capability. TLV 0x0206
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities entropy-label-capability <i>boolean</i>
Tree	entropy-label-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

graceful-restart-capability *boolean*

Description	Fault tolerance protection TLV 0x0503
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities graceful-restart-capability <i>boolean</i>
Tree	graceful-restart-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

make-before-break-capability *boolean*

Description	Make before break capability. TLV 0x050A
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities make-before-break-capability <i>boolean</i>
Tree	make-before-break-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

multipoint-to-multipoint-capability *boolean*

Description	Multipoint to multipoint FEC capability. TLV 0x0509
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities multipoint-to-multipoint-capability <i>boolean</i>
Tree	multipoint-to-multipoint-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

nokia-vendor-overload-capability *boolean*

Description	Overload capability
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities nokia-vendor-overload-capability <i>boolean</i>
Tree	nokia-vendor-overload-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

point-to-multipoint-capability *boolean*

Description	Point to multipoint FEC capability. TLV 0x0508
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities point-to-multipoint-capability <i>boolean</i>
Tree	point-to-multipoint-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

state-advertisement-control

Description	State advertisement control capability. TLV 0x050D
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities state-advertisement-control
Tree	state-advertisement-control
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-prefix-disable *boolean*

Description	Indicates desire to not receive IPv4 prefix FECs
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities state-advertisement-control ipv4-prefix-disable <i>boolean</i>
Tree	ipv4-prefix-disable
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv6-prefix-disable *boolean*

Description	Indicates desire to not receive IPv6 prefix FECs
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities state-advertisement-control ipv6-prefix-disable <i>boolean</i>
Tree	ipv6-prefix-disable
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

p2p-pseudowire-fec-128-disable *boolean*

Description	Indicates desire to not receive P2P PW FEC 128 FECs
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities state-advertisement-control p2p-pseudowire-fec-128-disable <i>boolean</i>
Tree	p2p-pseudowire-fec-128-disable
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

p2p-pseudowire-fec-129-disable *boolean*

Description	Indicates desire to not receive P2P PW FEC 129 FECs
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities state-advertisement-control p2p-pseudowire-fec-129-disable <i>boolean</i>
Tree	p2p-pseudowire-fec-129-disable
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

unrecognized-notification-capability *boolean*

Description	Unrecognized notification capability. TLV 0x0603
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> received-capabilities unrecognized-notification-capability <i>boolean</i>
Tree	unrecognized-notification-capability
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-holdtime

Description	Session holdtime state.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> session-holdtime
Tree	session-holdtime
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

negotiated *number*

Description	Negotiated holdtime.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> session-holdtime negotiated <i>number</i>
Tree	negotiated
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peer-proposed *number*

Description	Peer holdtime.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> session-holdtime peer-proposed <i>number</i>
Tree	peer-proposed
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

remaining *number*

Description	Remaining holdtime.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> session-holdtime remaining <i>number</i>
Tree	remaining
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-state *keyword*

Description	Representing the operational status of the LDP session.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> session-state <i>keyword</i>
Tree	session-state
Options	<ul style="list-style-type: none"> non-existent NON EXISTENT state. Transport disconnected.

- initialized
INITIALIZED state.
- openrec
OPENREC state.
- opensent
OPENSENT state.
- operational
OPERATIONAL state.

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Statistics objects.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics
Tree	statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

address-statistics

Description	Enter the address-statistics context
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics address-statistics
Tree	address-statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv4

Description	Enter the ipv4 context
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics address-statistics ipv4
Tree	ipv4
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

advertised-addresses *number*

Description	The number of IPv4 addresses advertised to a peer.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics address-statistics ipv4 advertised-addresses <i>number</i>
Tree	advertised-addresses
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

received-addresses *number*

Description	The number of IPv4 addresses received from a peer.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics address-statistics ipv4 received-addresses <i>number</i>
Tree	received-addresses
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fec-statistics

Description	Enter the fec-statistics context
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics fec-statistics
Tree	fec-statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-prefix

Description	Enter the ipv4-prefix context
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics fec-statistics ipv4-prefix
Tree	ipv4-prefix
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

advertised-fecs *number*

Description The number of advertised IPv4 prefix FECs to a single peer or all peers. In the overall summary the same FEC prefix advertised to multiple peers counts as 1.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [statistics fec-statistics ipv4-prefix advertised-fecs](#) *number*

Tree [advertised-fecs](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

received-fecs *number*

Description The number of received IPv4 prefix FECs from a single peer or all peers. In the overall summary the same FEC prefix from different peers counts as 1.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [statistics fec-statistics ipv4-prefix received-fecs](#) *number*

Tree [received-fecs](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

received-messages

Description Inbound statistics.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [statistics received-messages](#)

Tree [received-messages](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

address *number*

Description The number of address messages sent or received.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [statistics received-messages address](#) *number*

Tree	address
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

address-withdraw *number*

Description	The number of address-withdraw messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages address-withdraw <i>number</i>
Tree	address-withdraw
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

capability *number*

Description	The number of messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages capability <i>number</i>
Tree	capability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

initialization *number*

Description	The number of initialization messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages initialization <i>number</i>
Tree	initialization
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

keepalive *number*

Description	The number of keepalive messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages keepalive <i>number</i>
Tree	keepalive
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-abort-request *number*

Description	The number of label-abort-request messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages label-abort-request <i>number</i>
Tree	label-abort-request
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-mapping *number*

Description	The number of label-mapping messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages label-mapping <i>number</i>
Tree	label-mapping
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-release *number*

Description	The number of label-release messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics received-messages label-release <i>number</i>
Tree	label-release
Default	0
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

label-request *number*

Description The number of label-request messages sent or received.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [statistics](#) [received-messages](#) [label-request](#) [number](#)

Tree [label-request](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

label-withdraw *number*

Description The number of label-withdraw messages sent or received.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [statistics](#) [received-messages](#) [label-withdraw](#) [number](#)

Tree [label-withdraw](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

notification *number*

Description The number of messages sent or received.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [statistics](#) [received-messages](#) [notification](#) [number](#)

Tree [notification](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

total-messages *number*

Description The number of messages sent or received.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [statistics](#) [received-messages](#) [total-messages](#) [number](#)

Tree [total-messages](#)

Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sent-messages

Description	Outbound statistics.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages
Tree	sent-messages
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

address *number*

Description	The number of address messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages address <i>number</i>
Tree	address
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

address-withdraw *number*

Description	The number of address-withdraw messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages address-withdraw <i>number</i>
Tree	address-withdraw
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

capability *number*

Description	The number of messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages capability <i>number</i>

Tree	capability
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

initialization *number*

Description	The number of initialization messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages initialization <i>number</i>
Tree	initialization
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

keepalive *number*

Description	The number of keepalive messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages keepalive <i>number</i>
Tree	keepalive
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-abort-request *number*

Description	The number of label-abort-request messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages label-abort-request <i>number</i>
Tree	label-abort-request
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-mapping *number*

Description	The number of label-mapping messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages label-mapping <i>number</i>
Tree	label-mapping
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-release *number*

Description	The number of label-release messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages label-release <i>number</i>
Tree	label-release
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-request *number*

Description	The number of label-request messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages label-request <i>number</i>
Tree	label-request
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

label-withdraw *number*

Description	The number of label-withdraw messages sent or received.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics sent-messages label-withdraw <i>number</i>
Tree	label-withdraw
Default	0
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

notification *number*

Description The number of messages sent or received.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [statistics](#) [sent-messages](#) [notification](#) [number](#)

Tree [notification](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

total-messages *number*

Description The number of messages sent or received.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [statistics](#) [sent-messages](#) [total-messages](#) [number](#)

Tree [total-messages](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

tcp-transport

Description Enter the tcp-transport context

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [tcp-transport](#)

Tree [tcp-transport](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

local-address *string*

Description Local address.

Context [network-instance name](#) [string](#) [protocols](#) [ldp](#) [peers](#) [peer](#) [lsr-id](#) [string](#) [label-space-id](#) [number](#) [tcp-transport](#) [local-address](#) [string](#)

Tree [local-address](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

local-port *number*

Description Local port number.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [tcp-transport local-port](#) *number*

Tree [local-port](#)

Range 0 to 65535

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

remote-address *string*

Description Remote address.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [tcp-transport remote-address](#) *string*

Tree [remote-address](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

remote-port *number*

Description Remote port number.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [tcp-transport remote-port](#) *number*

Tree [remote-port](#)

Range 0 to 65535

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

trace-options

Description Configure event/packet tracing for one specific session.

Context [network-instance name](#) *string* [protocols ldp peers peer lsr-id](#) *string* [label-space-id](#) *number* [trace-options](#)

Tree [trace-options](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

trace *keyword*

Description Specifies the trace information to be captured.

Context [network-instance name](#) [string protocols](#) [ldp peers](#) [peer lsr-id](#) [string label-space-id](#) [number trace-options](#) [trace](#) *keyword*

Tree [trace](#)

Options

- all
Trace all events and packets
- events-all
Trace all events
- events-session
Trace session related events
- events-binding
Trace binding related events
- messages-all
Trace all LDP messages
- messages-all-detail
Trace all LDP messages with detailed output
- messages-initialization
Trace LDP Initialization packets
- messages-initialization-detail
Trace LDP Initialization packets with detailed output
- messages-keepalive
Trace LDP Keepalive packets
- messages-label
Trace LDP Label Mapping, Label Request, Label Abort Request, Label Withdraw and Label Release packets
- messages-label-detail
Trace LDP Label Mapping, Label Request, Label Abort Request, Label Withdraw and Label Release packets with detailed output

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

session-keepalive-holdtime *number*

Description	The time interval after which an inactive LDP session terminates and the corresponding TCP session closes. Inactivity is defined as not receiving LDP packets from the peer.
Context	network-instance name <i>string</i> protocols ldp peers session-keepalive-holdtime <i>number</i>
Tree	session-keepalive-holdtime
Range	45 to 3600
Default	180
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

session-keepalive-interval *number*

Description	The interval between successive transmissions of keepalive packets. Keepalive packets are only sent in the absence of other LDP packets transmitted over the LDP session.
Context	network-instance name <i>string</i> protocols ldp peers session-keepalive-interval <i>number</i>
Tree	session-keepalive-interval
Range	15 to 1200
Default	60
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

trace-options

Description	Configure event/packet tracing for all sessions (configured and dynamic).
Context	network-instance name <i>string</i> protocols ldp peers trace-options
Tree	trace-options
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

trace *keyword*

Description	Specifies the trace information to be captured.
--------------------	---

Context	network-instance name <i>string</i> protocols ldp peers trace-options trace keyword
Tree	trace
Options	<ul style="list-style-type: none"> • all Trace all events and packets • events-all Trace all events • events-session Trace session related events • events-binding Trace binding related events • messages-all Trace all LDP messages • messages-all-detail Trace all LDP messages with detailed output • messages-initialization Trace LDP Initialization packets • messages-initialization-detail Trace LDP Initialization packets with detailed output • messages-keepalive Trace LDP Keepalive packets • messages-label Trace LDP Label Mapping, Label Request, Label Abort Request, Label Withdraw and Label Release packets • messages-label-detail Trace LDP Label Mapping, Label Request, Label Abort Request, Label Withdraw and Label Release packets with detailed output
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	LDP instance level statistics
Context	network-instance name <i>string</i> protocols ldp statistics
Tree	statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fec-statistics

Description	Enter the fec-statistics context
Context	network-instance name <i>string</i> protocols ldp statistics fec-statistics
Tree	fec-statistics
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

ipv4-prefix

Description	Enter the ipv4-prefix context
Context	network-instance name <i>string</i> protocols ldp statistics fec-statistics ipv4-prefix
Tree	ipv4-prefix
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

advertised-fecs *number*

Description	The number of advertised IPv4 prefix FECs to a single peer or all peers. In the overall summary the same FEC prefix advertised to multiple peers counts as 1.
Context	network-instance name <i>string</i> protocols ldp statistics fec-statistics ipv4-prefix advertised-fecs <i>number</i>
Tree	advertised-fecs
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

received-fecs *number*

Description	The number of received IPv4 prefix FECs from a single peer or all peers. In the overall summary the same FEC prefix from different peers counts as 1.
Context	network-instance name <i>string</i> protocols ldp statistics fec-statistics ipv4-prefix received-fecs <i>number</i>
Tree	received-fecs
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

protocol-errors

Description	Enter the protocol-errors context
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors
Tree	protocol-errors
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-ldp-identifier *number*

Description	The number of notification messages sent to advise of a bad LDP identifier
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors bad-ldp-identifier <i>number</i>
Tree	bad-ldp-identifier
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-message-length *number*

Description	The number of notification messages sent to advise of a bad message length
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors bad-message-length <i>number</i>
Tree	bad-message-length
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-pdu-length *number*

Description	The number of notification messages sent to advise of a bad PDU length
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors bad-pdu-length <i>number</i>
Tree	bad-pdu-length
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-protocol-version *number*

Description	The number of notification messages sent to advise of a bad protocol version
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors bad-protocol-version <i>number</i>
Tree	bad-protocol-version
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

bad-tlv-length *number*

Description	The number of notification messages sent to advise of a bad TLV length
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors bad-tlv-length <i>number</i>
Tree	bad-tlv-length
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

malformed-tlv-value *number*

Description	The number of notification messages sent to advise of a malformed TLV value
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors malformed-tlv-value <i>number</i>
Tree	malformed-tlv-value
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

missing-message-parameters *number*

Description	The number of notification messages sent to advise of missing mandatory parameters
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors missing-message-parameters <i>number</i>
Tree	missing-message-parameters

Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-rejected-bad-keepalive-time *number*

Description	The number of notification messages sent to advise that a TCP connection was closed because the requested keepalive time is not acceptable
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors session-rejected-bad-keepalive-time <i>number</i>
Tree	session-rejected-bad-keepalive-time
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-rejected-no-hello *number*

Description	The number of notification messages sent to advise that a TCP connection was closed because there was no matching Hello adjacency
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors session-rejected-no-hello <i>number</i>
Tree	session-rejected-no-hello
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-rejected-parameters-adv-mode *number*

Description	The number of notification messages sent to advise that a TCP connection was closed because the requested label advertisement mode is not acceptable
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors session-rejected-parameters-adv-mode <i>number</i>
Tree	session-rejected-parameters-adv-mode
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-rejected-parameters-label-range *number*

Description	The number of notification messages sent to advise that a TCP connection was closed because the requested label range is not acceptable
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors session-rejected-parameters-label-range <i>number</i>
Tree	session-rejected-parameters-label-range
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

session-rejected-parameters-max-pdu-length *number*

Description	The number of notification messages sent to advise that a TCP connection was closed because the requested Maximum PDU Length is not acceptable
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors session-rejected-parameters-max-pdu-length <i>number</i>
Tree	session-rejected-parameters-max-pdu-length
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

unknown-message-type *number*

Description	The number of notification messages sent to advise of an unknown message type
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors unknown-message-type <i>number</i>
Tree	unknown-message-type
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

unknown-tlv *number*

Description	The number of notification messages sent to advise of an unknown TLV
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors unknown-tlv <i>number</i>
Tree	unknown-tlv

Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

unsupported-address-family *number*

Description	The number of notification messages sent to advise that a TCP connection was closed because the FEC type is not IPv4
Context	network-instance name <i>string</i> protocols ldp statistics protocol-errors unsupported-address-family <i>number</i>
Tree	unsupported-address-family
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sessions-terminated-holdtime-expiry *number*

Description	The total number of LDP sessions that were terminated due to keepalive holdtime expiry.
Context	network-instance name <i>string</i> protocols ldp statistics sessions-terminated-holdtime-expiry <i>number</i>
Tree	sessions-terminated-holdtime-expiry
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

total-discovery-interfaces *number*

Description	The total number of IP subinterfaces on which basic LDP discovery is active.
Context	network-instance name <i>string</i> protocols ldp statistics total-discovery-interfaces <i>number</i>
Tree	total-discovery-interfaces
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

total-hello-adjacencies *number*

Description	The total number of hello adjacencies that have been formed.
--------------------	--

Context	network-instance name <i>string</i> protocols ldp statistics total-hello-adjacencies <i>number</i>
Tree	total-hello-adjacencies
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

total-peers *number*

Description	The total number of LDP TCP sessions that are established.
Context	network-instance name <i>string</i> protocols ldp statistics total-peers <i>number</i>
Tree	total-peers
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

linux

Description	Enable the linux context
Context	network-instance name <i>string</i> protocols linux
Tree	linux
Configurable	True
Platforms	Supported on all platforms

export-neighbors *boolean*

Description	Export neighbors to linux routing table
Context	network-instance name <i>string</i> protocols linux export-neighbors <i>boolean</i>
Tree	export-neighbors
Default	true
Configurable	True
Platforms	Supported on all platforms

export-routes *boolean*

Description	Export routes to linux routing table
Context	network-instance name <i>string</i> protocols linux export-routes <i>boolean</i>
Tree	export-routes
Default	false

Configurable	True
Platforms	Supported on all platforms

import-routes *boolean*

Description	Import routes from linux routing table
Context	network-instance name <i>string</i> protocols linux import-routes <i>boolean</i>
Tree	import-routes
Default	false
Configurable	True
Platforms	Supported on all platforms

ospf

Description	Top-level configuration and operational state for Open Shortest Path First (OSPF)
Context	network-instance name <i>string</i> protocols ospf
Tree	ospf
Configurable	True
Platforms	Supported on all platforms

instance [name](#) *string*

Description	List of OSPF protocol instances associated with this network-instance.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i>
Tree	instance
Configurable	True
Platforms	Supported on all platforms
Max. Elements	3

name *string*

Description	The name of the OSPF instance
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

address-family *identityref*

Description	The address family that this instance supports. Only valid for OSPFv3.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> address-family <i>identityref</i>
Tree	address-family
Options	<ul style="list-style-type: none">• ipv6-unicast IPv6 unicast address family• ipv4-unicast IPv4 unicast address family
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Used to administratively enable or disable the OSPF instance
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none">• enable• disable
Configurable	True
Platforms	Supported on all platforms

advertise-router-capability *keyword*

Description	Scope to advertise router-capability.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> advertise-router-capability <i>keyword</i>
Tree	advertise-router-capability
Options	<ul style="list-style-type: none">• false• link• area• as
Configurable	True

Platforms Supported on all platforms

area *area-id*

Description The OSPF areas within which the local system exists

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#)

Tree [area](#)

Configurable True

Platforms Supported on all platforms

area-id

Description the area identifier as a dotted-quad.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#)

Configurable True

Platforms Supported on all platforms

active-interfaces *number*

Description The number of active interfaces in this area.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [active-interfaces](#) *number*

Tree [active-interfaces](#)

Configurable False

Platforms Supported on all platforms

advertise-router-capability *boolean*

Description Allow router advertisement capabilities

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [advertise-router-capability](#) *boolean*

Tree [advertise-router-capability](#)

Default true

Configurable True

Platforms Supported on all platforms

area-bdr-rtr-count

Description	The total number of area border routers reachable within this area.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id area-bdr-rtr-count
Tree	area-bdr-rtr-count
Configurable	False
Platforms	Supported on all platforms

area-range [ip-prefix-mask](#) (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the area-range context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id area-range ip-prefix-mask (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Tree	area-range
Configurable	True
Platforms	Supported on all platforms

ip-prefix-mask (*ipv4-prefix* | *ipv6-prefix*)

Description	ip-prefix with host bits set to 0
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id area-range ip-prefix-mask (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Configurable	True
Platforms	Supported on all platforms

advertise *boolean*

Description	Advertise summarized range of addresses to other areas
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id area-range ip-prefix-mask (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) advertise <i>boolean</i>
Tree	advertise
Default	true
Configurable	True
Platforms	Supported on all platforms

as-bdr-rtr-count

Description	The total number of autonomous system border routers reachable within this area.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id as-bdr-rtr-count
Tree	as-bdr-rtr-count
Configurable	False
Platforms	Supported on all platforms

blackhole-aggregate *boolean*

Description	Enables the creation of a blackhole for generated aggregates
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id blackhole-aggregate <i>boolean</i>
Tree	blackhole-aggregate
Default	true
Configurable	True
Platforms	Supported on all platforms

export-policy *reference*

Description	Apply an export policy when summarizing from this area to other areas.. Summary LSAs for prefixes matching the policy will still be in the linkstate database but are not flooded.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id export-policy <i>reference</i>
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

full-spf-runs

Description	The total number of times that complete SPF has been run on the router since OSPF was last enabled.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id full-spf-runs
Tree	full-spf-runs
Configurable	False

Platforms Supported on all platforms

interface [interface-name](#) *reference*

Description List of OSPF interfaces

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference*

Tree [interface](#)

Configurable True

Platforms Supported on all platforms

interface-name *reference*

Description Router logical interface name.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference*

Reference [network-instance name](#) *string* [interface name](#) *string*

Configurable True

Platforms Supported on all platforms

admin-state *keyword*

Description Administrative state of the OSPF

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [admin-state](#) *keyword*

Tree [admin-state](#)

Default enable

Options

- enable
- disable

Configurable True

Platforms Supported on all platforms

advertise-router-capability *boolean*

Description Allow router advertisement capabilities

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [advertise-router-capability](#) *boolean*

Tree [advertise-router-capability](#)

Default	true
Configurable	True
Platforms	Supported on all platforms

advertise-subnet *boolean*

Description	Advertise point-to-point interfaces as subnet routes
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> advertise-subnet <i>boolean</i>
Tree	advertise-subnet
Default	true
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Container with authentication options that apply to all peers in this peer-group
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

keychain *reference*

Description	Reference to a keychain. The keychain type must be ospf
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> authentication keychain <i>reference</i>
Tree	keychain
Reference	system authentication keychain name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

bad-packets

Description	Bad packets counters
--------------------	----------------------

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets
Tree	bad-packets
Configurable	False
Platforms	Supported on all platforms

auth-failures

Description	The total number of OSPF packets received with an invalid authorization key since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets auth-failures
Tree	auth-failures
Configurable	False
Platforms	Supported on all platforms

bad-area

Description	The total number of OSPF packets received with an area mismatch since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-area
Tree	bad-area
Configurable	False
Platforms	Supported on all platforms

bad-auth-type

Description	The total number of OSPF packets received with an invalid authorization type since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-auth-type
Tree	bad-auth-type
Configurable	False
Platforms	Supported on all platforms

bad-checksum

Description	The count of LS-as received with bad checksums.
--------------------	---

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-checksum
Tree	bad-checksum
Configurable	False
Platforms	Supported on all platforms

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'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-dead-interval
Tree	bad-dead-interval
Configurable	False
Platforms	Supported on all platforms

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'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-dest-address
Tree	bad-dest-address
Configurable	False
Platforms	Supported on all platforms

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'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-hello-interval
Tree	bad-hello-interval
Configurable	False
Platforms	Supported on all platforms

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'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-length
Tree	bad-length
Configurable	False
Platforms	Supported on all platforms

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'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-neighbors
Tree	bad-neighbors
Configurable	False
Platforms	Supported on all platforms

bad-network

Description	The total number of OSPF packets received with invalid network or mask since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-network
Tree	bad-network
Configurable	False
Platforms	Supported on all platforms

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'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> bad-packets bad-options
Tree	bad-options
Configurable	False

Platforms Supported on all platforms

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'.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [bad-packets bad-packet-type](#)

Tree [bad-packet-type](#)

Configurable False

Platforms Supported on all platforms

bad-version

Description The total number of OSPF packets received with bad OSPF version numbers since admin-state was last set to 'enabled'.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [bad-packets bad-version](#)

Tree [bad-version](#)

Configurable False

Platforms Supported on all platforms

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'.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [bad-packets bad-virtual-link](#)

Tree [bad-virtual-link](#)

Configurable False

Platforms Supported on all platforms

bdr-id

Description The value of bdr-id indicates the router ID of the backup designated router.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [bdr-id](#)

Tree [bdr-id](#)

Configurable False

Platforms Supported on all platforms

dead-interval *number*

Description Time OSPF waits without receiving Hello packets before declaring a neighbor down

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [dead-interval](#) *number*

Tree [dead-interval](#)

Range 2 to 65535

Default 40

Units seconds

Configurable True

Platforms Supported on all platforms

dr-id

Description The value of DR-id indicates the router ID of the designated router.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [dr-id](#)

Tree [dr-id](#)

Configurable False

Platforms Supported on all platforms

events

Description The value of events indicates the number of times this OSPF interface has changed its state, or an error has occurred.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [events](#)

Tree [events](#)

Configurable False

Platforms Supported on all platforms

failure-detection

Description Options related to methods of detecting BGP session failure

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> failure-detection
Tree	failure-detection
Configurable	True
Platforms	Supported on all platforms

enable-bfd *boolean*

Description	Enables the use of BFD for liveliness detection
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> failure-detection enable-bfd <i>boolean</i>
Tree	enable-bfd
Default	false
Configurable	True
Platforms	Supported on all platforms

hello-interval *number*

Description	Time between OSPF Hellos of this interface
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> hello-interval <i>number</i>
Tree	hello-interval
Range	1 to 65535
Default	10
Units	seconds
Configurable	True
Platforms	Supported on all platforms

interface-type *keyword*

Description	Interface type to broadcast or point-to-point
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> interface-type <i>keyword</i>
Tree	interface-type
Options	<ul style="list-style-type: none"> • broadcast • point-to-point
Configurable	True

Platforms Supported on all platforms

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.

Context [network-instance name string protocols ospf instance name string area area-id interface interface-name reference last-enabled-time](#)

Tree [last-enabled-time](#)

Configurable False

Platforms Supported on all platforms

last-event-time *string*

Description The value of last-event-time indicates the value of sys-up-time when an event was last associated with this OSPF interface.

Context [network-instance name string protocols ospf instance name string area area-id interface interface-name reference last-event-time string](#)

Tree [last-event-time](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

ldp-synchronization

Description Container with configuration options and state that pertains to the operation of LDP-IGP synchronization on this interface.

Context [network-instance name string protocols ospf instance name string area area-id interface interface-name reference ldp-synchronization](#)

Tree [ldp-synchronization](#)

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

disable

Description Disable LDP-IGP synchronization procedures on this interface, even if synchronization is enabled globally

Context [network-instance name string protocols ospf instance name string area area-id interface interface-name reference ldp-synchronization disable](#)

Tree	disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

duration *number*

Description	The length of time that the IGP interface has been in sync or out of sync
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> ldp-synchronization duration <i>number</i>
Tree	duration
Units	seconds
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

end-of-lib *boolean*

Description	<p>When set to true, the IGP restores the normal metric for the IGP adjacency when learning from LDP that all label-FEC mappings have been received from the LDP peer, even if there is remaining time on the hold-down-timer.</p> <p>When set to false, the IGP always waits for the full duration of the hold-down-timer to restore the normal metric for the IGP adjacency.</p> <p>This overrides the global/instance level setting.</p>
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> ldp-synchronization end-of-lib <i>boolean</i>
Tree	end-of-lib
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hold-down-timer *number*

Description	<p>The maximum amount of time that the IGP advertises a maximum metric for an interface, measured from the time that the LDP adjacency is re-established after going down.</p> <p>This overrides the global/instance level setting.</p>
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> ldp-synchronization hold-down-timer <i>number</i>
Tree	hold-down-timer
Range	1 to 1800

Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

sync-state *keyword*

Description	The current state of the interface with respect to LDP-IGP sync
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> ldp-synchronization sync-state <i>keyword</i>
Tree	sync-state
Options	<ul style="list-style-type: none"> • wait-for-LDP-adjacency The IGP is waiting for the LDP adjacency to come up. The interface is being advertised with max-metric. • hold-down-timer-active The LDP adjacency has come up and the IGP has started the hold-down-timer, waiting for either end-of-lib or hold-down-timer expiry. The interface is being advertised with max-metric. • end-of-lib-received The IGP received end-of-lib and has switched to normal operation. The interface is being advertised with a normal metric • hold-down-timer-expired The IGP did not receive end-of-lib (or was configured to ignore it) but hold-down-timer has expired and normal metric is restored. • manual-exit A tools command was performed to exit ldp-sync. Normal operation is resumed, max-metric is removed. • disabled ldp-sync is not applicable on this interface
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

link-lsa-cksum-sum *string*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> link-lsa-cksum-sum <i>string</i>

Tree	link-lsa-cksum-sum
Configurable	False
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> link-lsa-count
Tree	link-lsa-count
Configurable	False
Platforms	Supported on all platforms

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

Description	The value of local-ip-address indicates the IP address of this OSPF interface.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> local-ip-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	local-ip-address
Configurable	False
Platforms	Supported on all platforms

lsa-filter-out *keyword*

Description	LSA flooding reduction
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> lsa-filter-out <i>keyword</i>
Tree	lsa-filter-out
Default	none
Options	<ul style="list-style-type: none"> • none • all • except-own-rtrlsa • except-own-rtrlsa-and-defaults
Configurable	True
Platforms	Supported on all platforms

lsa-totals

Description	The number of LSAs of each type in this interface's database
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> lsa-totals
Tree	lsa-totals
Configurable	False
Platforms	Supported on all platforms

e-link-lsa

Description	The number of extended link LSAs in this interface's database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> lsa-totals e-link-lsa
Tree	e-link-lsa
Configurable	False
Platforms	Supported on all platforms

link-lsa

Description	The number of link LSAs in this interface's database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> lsa-totals link-lsa
Tree	link-lsa
Configurable	False
Platforms	Supported on all platforms

link-opaque-lsa

Description	The number of link opaque LSAs in this interface's database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> lsa-totals link-opaque-lsa
Tree	link-opaque-lsa
Configurable	False
Platforms	Supported on all platforms

router-info-lsa

Description	The number of link scoped router information LSAs in this interface's AS database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> lsa-totals router-info-lsa
Tree	router-info-lsa
Configurable	False
Platforms	Supported on all platforms

metric number

Description	Explicit route cost metric that is applied to the interface
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> metric number
Tree	metric
Configurable	True
Platforms	Supported on all platforms

mtu number

Description	MTU for the OSPF to use on the interface. For OSPFv3 this must be minimum 1280. If the MTU defined here exceeds the actual IP-MTU of the interface, then the IP-MTU of the interface is used.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> mtu number
Tree	mtu
Range	512 to 9486
Configurable	True
Platforms	Supported on all platforms

neighbor [router-id](#)

Description	List of neighbors associated with this OSPF interface
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id
Tree	neighbor
Configurable	False
Platforms	Supported on all platforms

router-id

Description	The router-id advertised by the neighbor
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id
Configurable	False
Platforms	Supported on all platforms

address (*ipv4-address* | *ipv6-address-with-zone*)

Description	The value of address indicates the IP address of the neighbor associated with the local link.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Tree	address
Configurable	False
Platforms	Supported on all platforms

adjacency-state *identityref*

Description	Current OSPF Neighbor state
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id adjacency-state identityref
Tree	adjacency-state
Options	<ul style="list-style-type: none"> • down <p>The initial state of a neighbor, indicating that no recent information has been received from the neighbor.</p> • attempt <p>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.</p> • init <p>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.</p> • 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 primary/standby 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
Platforms	Supported on all platforms

backup-designated-router

Description	Advertised backup designated router
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id backup-designated-router
Tree	backup-designated-router
Configurable	False
Platforms	Supported on all platforms

dead-time *number*

Description	The remaining number of seconds remaining in the neighbor's dead time interval
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id dead-time <i>number</i>
Tree	dead-time
Configurable	False
Platforms	Supported on all platforms

designated-router

Description	Advertised designated router
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id designated-router
Tree	designated-router
Configurable	False
Platforms	Supported on all platforms

last-established-time *number*

Description	Time then OSPF neighbor was last established
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id last-established-time <i>number</i>
Tree	last-established-time
Configurable	False
Platforms	Supported on all platforms

last-event-time

Description	The value of last-event-time indicates the value of sys-up-time when the last event occurred that affected the adjacency to the neighbour.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id last-event-time
Tree	last-event-time
Configurable	False
Platforms	Supported on all platforms

last-restart-time

Description	the value of last-restart-time indicates the last time the neighbor attempted restart.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id last-restart-time
Tree	last-restart-time
Configurable	False
Platforms	Supported on all platforms

optional-capabilities

Description	Advertised Optional Capabilities
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id optional-capabilities
Tree	optional-capabilities
Configurable	False
Platforms	Supported on all platforms

priority *number*

Description	Router priority advertised by neighbor
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id priority <i>number</i>
Tree	priority
Configurable	False
Platforms	Supported on all platforms

restart-helper-age *number*

Description	The value of restart-helper-age indicates the remaining time in the current OSPF graceful restart interval, if the router is acting as a restart helper for the neighbor.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id restart-helper-age <i>number</i>
Tree	restart-helper-age
Range	0 to 1800
Units	seconds
Configurable	False
Platforms	Supported on all platforms

restart-helper-exit-rc *keyword*

Description	the value of restart-helper-exit-rc indicates the outcome of the last attempt at acting as a graceful restart helper for the neighbor. none no restart has yet been attempted. in-progress A restart attempt is currently underway. completed the last restart completed successfully. timed-out the last restart timed out. topology-changed the last restart was aborted due to a topology change.
--------------------	--

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id restart-helper-exit-rc <i>keyword</i>
Tree	restart-helper-exit-rc
Options	<ul style="list-style-type: none"> • none • in-progress • completed • timed-out • topology-changed • bfd-down
Configurable	False
Platforms	Supported on all platforms

restart-helper-status *keyword*

Description	The value of restart-helper-status indicates whether the router is acting as a graceful restart helper for the neighbor.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id restart-helper-status <i>keyword</i>
Tree	restart-helper-status
Options	<ul style="list-style-type: none"> • not-helping • helping
Configurable	False
Platforms	Supported on all platforms

restart-reason (*number* | *keyword*)

Description	The value of restart-reason indicates the OSPF neighbor's graceful restart reason.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id restart-reason (<i>number</i> <i>keyword</i>)
Tree	restart-reason
Range	4 to 4294967295
Options	<ul style="list-style-type: none"> • unknown • sw-restart • sw-reload

	<ul style="list-style-type: none"> switch-red
Configurable	False
Platforms	Supported on all platforms

retransmission-queue-length *number*

Description	Enter the retransmission-queue-length context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id retransmission-queue-length <i>number</i>
Tree	retransmission-queue-length
Configurable	False
Platforms	Supported on all platforms

state-changes *number*

Description	Total numer of OSPF state changes
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id state-changes <i>number</i>
Tree	state-changes
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

bad-mtu

Description	The value of bad-MT-us indicates the total number of times when the MTU in a received database description packet was larger than the MTU of the receiving interface since admin-state was last set to 'enabled'.
--------------------	---

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics bad-mtu
Tree	bad-mtu
Configurable	False
Platforms	Supported on all platforms

bad-nbr-states

Description	The value of bad-nbr-states indicates the total number of OSPF packets received when the neighbor state was not expecting to receive this packet type since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics bad-nbr-states
Tree	bad-nbr-states
Configurable	False
Platforms	Supported on all platforms

bad-packets

Description	The value of bad-packets indicates the total number of times when an LS update was received with an illegal LS type or an option mismatch since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics bad-packets
Tree	bad-packets
Configurable	False
Platforms	Supported on all platforms

bad-seq-nums

Description	The value of bad-seq-nums indicates the total number of times when a database description packet was received with a sequence number mismatch since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics bad-seq-nums
Tree	bad-seq-nums
Configurable	False

Platforms Supported on all platforms

duplicates

Description The value of duplicates indicates the total number of times when a duplicate database description packet was received during the exchange state since admin-state was last set to 'enabled'.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [neighbor router-id statistics duplicates](#)

Tree [duplicates](#)

Configurable False

Platforms Supported on all platforms

events

Description The value of events indicates the number of times this neighbor relationship has changed state, or an error has occurred.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [neighbor router-id statistics events](#)

Tree [events](#)

Configurable False

Platforms Supported on all platforms

Isa-install-failed

Description The value of Isa-install-failed indicates the total number of times an LSA could not be installed into the LSDB due to a resource allocation issue since admin-state was last set to 'enabled'.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id interface interface-name](#) *reference* [neighbor router-id statistics Isa-install-failed](#)

Tree [Isa-install-failed](#)

Configurable False

Platforms Supported on all platforms

Isa-not-in-lsdb

Description The value of Isa-not-in-lsdb indicates the total number of times when an LS request was received for an LSA not installed in the LSDB of this router since admin-state was last set to 'enabled'.

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics lsa-not-in-lsdb
Tree	lsa-not-in-lsdb
Configurable	False
Platforms	Supported on all platforms

num-restarts

Description	The value of num-restarts indicates the number of times the neighbor has attempted restart.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics num-restarts
Tree	num-restarts
Configurable	False
Platforms	Supported on all platforms

option-mismatches

Description	The value of option-mismatches indicates the total number of times when a LS update was received with an option mismatch since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id statistics option-mismatches
Tree	option-mismatches
Configurable	False
Platforms	Supported on all platforms

up-time *number*

Description	The value of up-time indicates the uninterrupted time, in hundredths of seconds, the adjacency to this neighbour has been up.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> neighbor router-id up-time <i>number</i>
Tree	up-time
Range	0 to 2147483647
Units	centiseconds
Configurable	False

Platforms Supported on all platforms

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'.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [neighbor-count](#)

Tree [neighbor-count](#)

Configurable False

Platforms Supported on all platforms

oper-state *keyword*

Description The OSPF interface state.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [oper-state](#) *keyword*

Tree [oper-state](#)

Options

- down
- loopback
- waiting
- point-to-point
- designated-router
- backup-designated-router
- other-designated-router

Configurable False

Platforms Supported on all platforms

packets

Description Packet counters

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [area area-id](#) [interface interface-name](#) *reference* [packets](#)

Tree [packets](#)

Configurable False

Platforms Supported on all platforms

discarded

Description	The total number of OSPF packets discarded since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets discarded
Tree	discarded
Configurable	False
Platforms	Supported on all platforms

retransmits

Description	The total number of OSPF retransmits since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets retransmits
Tree	retransmits
Configurable	False
Platforms	Supported on all platforms

rx-db-description

Description	The total number of OSPF database description packets received since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets rx-db-description
Tree	rx-db-description
Configurable	False
Platforms	Supported on all platforms

rx-hello

Description	The total number of OSPF hello packets received since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets rx-hello
Tree	rx-hello
Configurable	False
Platforms	Supported on all platforms

rx-ls-ack

Description	The total number of link state acknowledgements received since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets rx-ls-ack
Tree	rx-ls-ack
Configurable	False
Platforms	Supported on all platforms

rx-ls-request

Description	The total number of link state requests (LS-rs) received since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets rx-ls-request
Tree	rx-ls-request
Configurable	False
Platforms	Supported on all platforms

rx-ls-update

Description	The total number of link state updates (LS-us) received since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets rx-ls-update
Tree	rx-ls-update
Configurable	False
Platforms	Supported on all platforms

rx-total

Description	The total number of OSPF packets received since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets rx-total
Tree	rx-total
Configurable	False
Platforms	Supported on all platforms

tx-db-description

Description	The total number of OSPF database description packets transmitted since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets tx-db-description
Tree	tx-db-description
Configurable	False
Platforms	Supported on all platforms

tx-hello

Description	The total number of OSPF hello packets transmitted since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets tx-hello
Tree	tx-hello
Configurable	False
Platforms	Supported on all platforms

tx-ls-ack

Description	The total number of OSPF link state acknowledgements transmitted since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets tx-ls-ack
Tree	tx-ls-ack
Configurable	False
Platforms	Supported on all platforms

tx-ls-request

Description	The total number of OSPF link state requests (LS-rs) transmitted since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets tx-ls-request
Tree	tx-ls-request
Configurable	False
Platforms	Supported on all platforms

tx-ls-update

Description	The total number of OSPF link state updates (LS-us) transmitted since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets tx-ls-update
Tree	tx-ls-update
Configurable	False
Platforms	Supported on all platforms

tx-total

Description	The total number of OSPF packets transmitted since admin-state was last set to 'enabled'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> packets tx-total
Tree	tx-total
Configurable	False
Platforms	Supported on all platforms

passive *boolean*

Description	Allow interface to be advertised as an OSPF interface without running the OSPF protocol
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> passive boolean
Tree	passive
Configurable	True
Platforms	Supported on all platforms

priority *number*

Description	Priority of the interface to apply in the designated router election on the subnet
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> priority number
Tree	priority
Range	0 to 255
Default	1

Configurable	True
Platforms	Supported on all platforms

retransmit-interval *number*

Description	Time before OSPF retransmits an unacknowledged LSA to a neighbor
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> retransmit-interval <i>number</i>
Tree	retransmit-interval
Range	1 to 1800
Default	5
Units	seconds
Configurable	True
Platforms	Supported on all platforms

trace-options

Description	Enter the trace-options context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace

Description	Tracing parameter flags
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace
Tree	trace
Configurable	True
Platforms	Supported on all platforms

adjacencies

Description	Enable tracing all BGP events.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace adjacencies

Tree	adjacencies
Configurable	True
Platforms	Supported on all platforms

interfaces

Description	Enable tracing all interface events.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace interfaces
Tree	interfaces
Configurable	True
Platforms	Supported on all platforms

packet

Description	Trace OSPF Packet types Only one type can be enabled at a time
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace packet
Tree	packet
Configurable	True
Platforms	Supported on all platforms

detail

Description	To enable detailed tracing. Includes both received and sent packets.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace packet detail
Tree	detail
Configurable	True
Platforms	Supported on all platforms

modifier *keyword*

Description	Enter the modifier context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace packet modifier keyword
Tree	modifier

Options	<ul style="list-style-type: none"> • ingress To enable tracing for the packets which are received. • egress To enable tracing for the sent packets. • in-and-egress To enable tracing for both sent and received packets • drop To enable tracing for the sent packets.
Configurable	True
Platforms	Supported on all platforms

type *keyword*

Description	Enter the type context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> trace-options trace packet type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • all Enable tracing of all OSPF packets • hello Enable tracing of OSPF Hello packets • dbdescr Enable tracing of OSPF database Descriptor packets • ls-request Enable tracing of OSPF link-state request packets • ls-update Enable tracing of OSPF link-state update packets • ls-ack Enable tracing of OSPF link-state Ack packets
Configurable	True
Platforms	Supported on all platforms

transit-delay *number*

Description	Time required to transmit an LSA on the interface, virtual link, or sham link
--------------------	---

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> transit-delay <i>number</i>
Tree	transit-delay
Range	1 to 1800
Default	1
Units	seconds
Configurable	True
Platforms	Supported on all platforms

type *keyword*

Description	The value of type indicates the operational OSPF interface type.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>reference</i> type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • broadcast • point-to-point
Configurable	False
Platforms	Supported on all platforms

last-spf-run-time

Description	The sys-up-time when intra-area SPF was last run on this area.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id last-spf-run-time
Tree	last-spf-run-time
Configurable	False
Platforms	Supported on all platforms

lsa-filter-totals

Description	The number of LSAs not sent due to area policy.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-filter-totals
Tree	lsa-filter-totals
Configurable	False
Platforms	Supported on all platforms

export-filtered

Description	The number of LSAs not sent due to area export policy.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-filter-totals export-filtered
Tree	export-filtered
Configurable	False
Platforms	Supported on all platforms

import-filtered

Description	The number of LSAs not sent due to area import policy.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-filter-totals import-filtered
Tree	import-filtered
Configurable	False
Platforms	Supported on all platforms

lsa-totals

Description	The number of LSAs of each type in this area's database
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals
Tree	lsa-totals
Configurable	False
Platforms	Supported on all platforms

area-opaque-lsa

Description	The number of NSSA LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals area-opaque-lsa
Tree	area-opaque-lsa
Configurable	False
Platforms	Supported on all platforms

asbr-summary-lsa

Description	The number of ASBR summary LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals asbr-summary-lsa
Tree	asbr-summary-lsa
Configurable	False
Platforms	Supported on all platforms

e-inter-area-prefix-lsa

Description	The number of OSPFv3 E-inter-area-prefix LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals e-inter-area-prefix-lsa
Tree	e-inter-area-prefix-lsa
Configurable	False
Platforms	Supported on all platforms

e-inter-area-router-lsa

Description	The number of OSPFv3 E-inter-area-router LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals e-inter-area-router-lsa
Tree	e-inter-area-router-lsa
Configurable	False
Platforms	Supported on all platforms

e-intra-area-prefix-lsa

Description	The number of OSPFv3 E-intra-area-prefix LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals e-intra-area-prefix-lsa
Tree	e-intra-area-prefix-lsa
Configurable	False
Platforms	Supported on all platforms

e-network-lsa

Description	The number of OSPFv3 E-network LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals e-network-lsa
Tree	e-network-lsa
Configurable	False
Platforms	Supported on all platforms

e-nssa-lsa

Description	The number of OSPFv3 E-NSSA LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals e-nssa-lsa
Tree	e-nssa-lsa
Configurable	False
Platforms	Supported on all platforms

e-router-lsa

Description	The number of OSPFv3 E-router LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals e-router-lsa
Tree	e-router-lsa
Configurable	False
Platforms	Supported on all platforms

inter-area-prefix-lsa

Description	The number of OSPFv3 inter-area-prefix LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals inter-area-prefix-lsa
Tree	inter-area-prefix-lsa
Configurable	False
Platforms	Supported on all platforms

inter-area-router-lsa

Description	The number of OSPFv3 inter-area-router LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals inter-area-router-lsa
Tree	inter-area-router-lsa
Configurable	False
Platforms	Supported on all platforms

intra-area-prefix-lsa

Description	The number of OSPFv3 intra-area-prefix LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals intra-area-prefix-lsa
Tree	intra-area-prefix-lsa
Configurable	False
Platforms	Supported on all platforms

network-lsa

Description	The number of network LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals network-lsa
Tree	network-lsa
Configurable	False
Platforms	Supported on all platforms

network-summary-lsa

Description	The number of network summary LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals network-summary-lsa
Tree	network-summary-lsa
Configurable	False
Platforms	Supported on all platforms

nssa-lsa

Description	The number of NSSA LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals nssa-lsa
Tree	nssa-lsa
Configurable	False
Platforms	Supported on all platforms

router-info-lsa

Description	The number of OSPFv3 router-info LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals router-info-lsa
Tree	router-info-lsa
Configurable	False
Platforms	Supported on all platforms

router-lsa

Description	The number of router LSAs in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals router-lsa
Tree	router-lsa
Configurable	False
Platforms	Supported on all platforms

total

Description	The number of area scope LSAs within this area.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals total
Tree	total
Configurable	False
Platforms	Supported on all platforms

total-lsa-cksum-sum *string*

Description	The 32-bit unsigned sum of the area scope LSA checksums contained in this area'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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals total-lsa-cksum-sum <i>string</i>
Tree	total-lsa-cksum-sum
Configurable	False
Platforms	Supported on all platforms

unknown-lsa

Description	The number of unknown LSA advertisements in this area's link-state database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id lsa-totals unknown-lsa
Tree	unknown-lsa
Configurable	False
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa
Tree	nssa
Configurable	True
Platforms	Supported on all platforms

area-range [ip-prefix-mask](#) (*ipv4-prefix | ipv6-prefix*)

Description	Enter the area-range context
--------------------	------------------------------

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa area-range ip-prefix-mask (<i>ipv4-prefix ipv6-prefix</i>)
Tree	area-range
Configurable	True
Platforms	Supported on all platforms

ip-prefix-mask (*ipv4-prefix | ipv6-prefix*)

Description	ip-prefix with host bits set to 0
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa area-range ip-prefix-mask (<i>ipv4-prefix ipv6-prefix</i>)
Configurable	True
Platforms	Supported on all platforms

advertise *boolean*

Description	Advertise summarized range of addresses to other areas
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa area-range ip-prefix-mask (<i>ipv4-prefix ipv6-prefix</i>) advertise <i>boolean</i>
Tree	advertise
Default	true
Configurable	True
Platforms	Supported on all platforms

originate-default-route

Description	Enter the originate-default-route context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa originate-default-route
Tree	originate-default-route
Configurable	True
Platforms	Supported on all platforms

adjacency-check *boolean*

Description	Default route to remove if there is no adjacency
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa originate-default-route adjacency-check <i>boolean</i>

Tree	adjacency-check
Default	true
Configurable	True
Platforms	Supported on all platforms

type-nssa *boolean*

Description	Generate a default route using NSSA-LSA type
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa originate-default-route type-nssa <i>boolean</i>
Tree	type-nssa
Default	false
Configurable	True
Platforms	Supported on all platforms

redistribute-external *boolean*

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
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa redistribute-external <i>boolean</i>
Tree	redistribute-external
Default	true
Configurable	True
Platforms	Supported on all platforms

summaries *boolean*

Description	Enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR)
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id nssa summaries <i>boolean</i>
Tree	summaries
Default	true
Configurable	True
Platforms	Supported on all platforms

stub

Description	Enable the stub context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id <i>stub</i>
Tree	stub
Configurable	True
Platforms	Supported on all platforms

default-metric *number*

Description	Defines the default OSPF metric for associated stub area
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id <i>stub</i> default-metric <i>number</i>
Tree	default-metric
Range	1 to 65535
Default	1
Configurable	True
Platforms	Supported on all platforms

summaries *boolean*

Description	Enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR)
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id <i>stub</i> summaries <i>boolean</i>
Tree	summaries
Default	true
Configurable	True
Platforms	Supported on all platforms

area-border-router *boolean*

Description	This indicates whether this router is an area border router.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area-border-router <i>boolean</i>
Tree	area-border-router
Configurable	False
Platforms	Supported on all platforms

as-border-router *boolean*

Description	This indicates whether this router is an AS border router.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> as-border-router <i>boolean</i>
Tree	as-border-router
Configurable	False
Platforms	Supported on all platforms

asbr

Description	Configure the router as an ASBR (Autonomous System Boundary Router)
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> asbr
Tree	asbr
Configurable	True
Platforms	Supported on all platforms

trace-path (*number* | *keyword*)

Description	Domain identity
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> asbr trace-path (<i>number</i> <i>keyword</i>)
Tree	trace-path
Range	0 to 31
Default	none
Options	<ul style="list-style-type: none"> • none
Configurable	True
Platforms	Supported on all platforms

backbone-router *boolean*

Description	This indicates whether or not this router is configured as an OSPF back bone router.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> backbone-router <i>boolean</i>
Tree	backbone-router
Configurable	False

Platforms Supported on all platforms

export-limit

Description Enter the export-limit context

Context [network-instance name string protocols ospf instance name string export-limit](#)

Tree [export-limit](#)

Configurable True

Platforms Supported on all platforms

log-percent *number*

Description Export limit at which warning a log message and SNMP notification are sent

Context [network-instance name string protocols ospf instance name string export-limit log-percent number](#)

Tree [log-percent](#)

Range 1 to 100

Configurable True

Platforms Supported on all platforms

number *number*

Description Maximum number of routes or prefixes to be exported into IGP instance from route table

Context [network-instance name string protocols ospf instance name string export-limit number number](#)

Tree [number](#)

Range 1 to 4294967295

Configurable True

Platforms Supported on all platforms

export-policy *reference*

Description Apply an export policy to redistribute routes into OSPF

Context [network-instance name string protocols ospf instance name string export-policy reference](#)

Tree [export-policy](#)

Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

extern-lsa-cksum-sum *string*

Description	The value of extern-lsa-cksum-sum indicates the 32-bit unsigned sum of the LS checksums of the external link-state advertisements contained in the link-state database. This 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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> extern-lsa-cksum-sum <i>string</i>
Tree	extern-lsa-cksum-sum
Configurable	False
Platforms	Supported on all platforms

extern-lsa-count

Description	The value of extern-lsa-count indicates the number of external LS-as (LS type 0x4005) in the link-state database
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> extern-lsa-count
Tree	extern-lsa-count
Configurable	False
Platforms	Supported on all platforms

external-db-overflow

Description	Enable the external-db-overflow context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> external-db-overflow
Tree	external-db-overflow
Configurable	True
Platforms	Supported on all platforms

interval *number*

Description	Enter the interval context
--------------------	----------------------------

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> external-db-overflow interval <i>number</i>
Tree	interval
Range	0 to 2147483647
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

limit *number*

Description	Enter the limit context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> external-db-overflow limit <i>number</i>
Tree	limit
Range	0 to 2147483647
Default	0
Configurable	True
Platforms	Supported on all platforms

external-preference *number*

Description	Configure the route preference associated with OSPF external routes
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> external-preference <i>number</i>
Tree	external-preference
Default	150
Configurable	True
Platforms	Supported on all platforms

graceful-restart

Description	Container for options related to OSPF graceful restart
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> graceful-restart
Tree	graceful-restart
Configurable	True

Platforms Supported on all platforms

helper-mode *boolean*

Description Enable or disable the OSPF graceful restart helper function. When this leaf is set, the local system supports retaining forwarding information during a neighbor router's restart.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [graceful-restart helper-mode](#) *boolean*

Tree [helper-mode](#)

Default false

Configurable True

Platforms Supported on all platforms

strict-lsa-checking *boolean*

Description Enter the strict-lsa-checking context

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [graceful-restart strict-lsa-checking](#) *boolean*

Tree [strict-lsa-checking](#)

Default false

Configurable True

Platforms Supported on all platforms

instance-id *number*

Description The OSPF multi instance identity as defined in RFC6549 or RFC5838. Supported values are: For OSPFv2 it is between 0 and 31, default is 0. For OSPFv3 address-family ipv6-unicast it is between 0 and 31, default is 0. For OSPFv3 address-family ipv4-unicast it is between 64 and 95, default is 64.

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [instance-id](#) *number*

Tree [instance-id](#)

Range 0 to 255

Configurable True

Platforms Supported on all platforms

last-disabled-reason *string*

Description	Reason why the disabled state was entered the last time.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-disabled-reason <i>string</i>
Tree	last-disabled-reason
String Length	0 to 20
Configurable	False
Platforms	Supported on all platforms

last-enabled-time *string*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-enabled-time <i>string</i>
Tree	last-enabled-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-overflow-entered-time *string*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-overflow-entered-time <i>string</i>
Tree	last-overflow-entered-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-overflow-exit-time *string*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-overflow-exit-time <i>string</i>
Tree	last-overflow-exit-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-overload-enter-code *keyword*

Description	The value of last-overload-enter-code indicates the condition which caused OSPF to get into overload.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-overload-enter-code <i>keyword</i>
Tree	last-overload-enter-code
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
Platforms	Supported on all platforms

last-overload-entered-time *string*

Description	The value of last-overload-entrd-time indicates the time at which the system last went into overload state.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-overload-entered-time <i>string</i>
Tree	last-overload-entered-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-overload-exit-code *keyword*

Description	The value of last-overload-exit-code indicates the reason why OSPF came out of overload state the last time, since reset.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-overload-exit-code <i>keyword</i>
Tree	last-overload-exit-code
Options	<ul style="list-style-type: none"> • none • bgp-sig-recv • timer-expired • manual-exit • sfm-overload-done
Configurable	False
Platforms	Supported on all platforms

last-overload-exit-time *string*

Description	The value of last-overload-exit-time indicates the time at which the system last came out of overload state.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> last-overload-exit-time <i>string</i>
Tree	last-overload-exit-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

ldp-synchronization

Description	Enable LDP-IGP synchronization procedures on all P2P interfaces and all LAN interfaces with a single adjacency, except on interfaces where the functionality is explicitly disabled.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> ldp-synchronization
Tree	ldp-synchronization
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

end-of-lib *boolean*

Description	When set to true, the IGP restores the normal metric for the IGP adjacency when learning from LDP that all label-FEC mappings have been received from the LDP peer, even if there is remaining time on the hold-down-timer. When set to false, the IGP always waits for the full duration of the hold-down-timer to restore the normal metric for the IGP adjacency.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> ldp-synchronization end-of-lib <i>boolean</i>
Tree	end-of-lib
Default	false
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

hold-down-timer *number*

Description	The maximum amount of time that the IGP advertises a maximum metric for an interface, measured from the time that the LDP adjacency is re-established after going down.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> ldp-synchronization hold-down-timer <i>number</i>
Tree	hold-down-timer
Range	1 to 1800
Default	60
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

lsa-totals

Description	The number of LSAs of each type in this instance's AS database
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> lsa-totals
Tree	lsa-totals
Configurable	False
Platforms	Supported on all platforms

as-external-lsa

Description	The number of AS External LSAs in this instance's AS database.
--------------------	--

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> lsa-totals as-external-lsa
Tree	as-external-lsa
Configurable	False
Platforms	Supported on all platforms

as-opaque-lsa

Description	The number of AS opaque LSAs in this instance's AS database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> lsa-totals as-opaque-lsa
Tree	as-opaque-lsa
Configurable	False
Platforms	Supported on all platforms

e-as-external-lsa

Description	The number of extended AS External LSAs in this instance's AS database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> lsa-totals e-as-external-lsa
Tree	e-as-external-lsa
Configurable	False
Platforms	Supported on all platforms

router-info-lsa

Description	The number of AS scoped router information LSAs in this instance's AS database.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> lsa-totals router-info-lsa
Tree	router-info-lsa
Configurable	False
Platforms	Supported on all platforms

max-ecmp-paths *number*

Description	The maximum number of ECMP next-hops to program into the FIB for every IP prefix
--------------------	--

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> max-ecmp-paths <i>number</i>
Tree	max-ecmp-paths
Range	1 to 64
Default	1
Configurable	True
Platforms	Supported on all platforms

new-lsas-originated

Description	The number of new link-state advertisements that have been originated. This number is incremented each time the router originates a new LSA.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> new-lsas-originated
Tree	new-lsas-originated
Configurable	False
Platforms	Supported on all platforms

new-lsas-received

Description	The number of link-state advertisements received determined to be new instantiations. This number does not include newer instantiations of self-originated link-state advertisements.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> new-lsas-received
Tree	new-lsas-received
Configurable	False
Platforms	Supported on all platforms

opaque-lsa-support *boolean*

Description	The value of opaque-lsa-support indicates the router's support for opaque LSA types. this object is valid only when version is 'version2'.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> opaque-lsa-support <i>boolean</i>
Tree	opaque-lsa-support
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	Used to report operational state of the OSPF instance
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	False
Platforms	Supported on all platforms

overflow *boolean*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overflow <i>boolean</i>
Tree	overflow
Configurable	False
Platforms	Supported on all platforms

overload

Description	Enter the overload context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload
Tree	overload
Configurable	True
Platforms	Supported on all platforms

active *boolean*

Description	Enter the active context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload active <i>boolean</i>
Tree	active
Default	false
Configurable	True

Platforms Supported on all platforms

overload-include-ext-1 *boolean*

Description Enter the overload-include-ext-1 context

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [overload-overload-include-ext-1](#) *boolean*

Tree [overload-include-ext-1](#)

Default false

Configurable True

Platforms Supported on all platforms

overload-include-ext-2 *boolean*

Description Enter the overload-include-ext-2 context

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [overload-overload-include-ext-2](#) *boolean*

Tree [overload-include-ext-2](#)

Default false

Configurable True

Platforms Supported on all platforms

overload-include-stub *boolean*

Description Enter the overload-include-stub context

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [overload-overload-include-stub](#) *boolean*

Tree [overload-include-stub](#)

Default false

Configurable True

Platforms Supported on all platforms

overload-on-boot

Description Enable the overload-on-boot context

Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [overload-overload-on-boot](#)

Tree [overload-on-boot](#)

Configurable	True
Platforms	Supported on all platforms

timeout *number*

Description	Enter the timeout context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload overload-on-boot timeout <i>number</i>
Tree	timeout
Range	60 to 1800
Default	60
Units	seconds
Configurable	True
Platforms	Supported on all platforms

rtr-adv-lsa-limit

Description	Enter the rtr-adv-lsa-limit context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload rtr-adv-lsa-limit
Tree	rtr-adv-lsa-limit
Configurable	True
Platforms	Supported on all platforms

log-only *boolean*

Description	Enter the log-only context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload rtr-adv-lsa-limit log-only <i>boolean</i>
Tree	log-only
Configurable	True
Platforms	Supported on all platforms

max-lsa-count *number*

Description	Enter the max-lsa-count context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload rtr-adv-lsa-limit max-lsa-count <i>number</i>

Tree	max-lsa-count
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

overload-timeout *number*

Description	Enter the overload-timeout context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload rtr-adv-lsa-limit overload-timeout <i>number</i>
Tree	overload-timeout
Range	1 to 1800
Configurable	True
Platforms	Supported on all platforms

warning-threshold *number*

Description	Enter the warning-threshold context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload rtr-adv-lsa-limit warning-threshold <i>number</i>
Tree	warning-threshold
Range	0 to 100
Default	0
Configurable	True
Platforms	Supported on all platforms

overload-rem-interval *number*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload-rem-interval <i>number</i>
Tree	overload-rem-interval
Range	0 to 65535
Units	seconds
Configurable	False
Platforms	Supported on all platforms

overload-state *keyword*

Description	The value of overload-oper-state indicates whether or not the OSPF application is presently in overload state or not.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload-state <i>keyword</i>
Tree	overload-state
Options	<ul style="list-style-type: none"> • overload • no-overload
Configurable	False
Platforms	Supported on all platforms

ovld-lsa-limit-rem-interval *number*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> ovld-lsa-limit-rem-interval <i>number</i>
Tree	ovld-lsa-limit-rem-interval
Range	0 to 65535
Units	seconds
Configurable	False
Platforms	Supported on all platforms

preference *number*

Description	Sets the route preference for OSPF sourced routes
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> preference <i>number</i>
Tree	preference
Range	1 to 255
Default	10
Configurable	True
Platforms	Supported on all platforms

reference-bandwidth *number*

Description	Configures the reference bandwidth that provides the basis for interface metrics based on link Bandwidth If the reference bandwidth is defined, then the cost is calculated using the following formula: $\text{cost} = \text{reference-bandwidth} / \text{bandwidth}$ 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, OSPF automatically reverts to the maximum configurable cost metric.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> reference-bandwidth <i>number</i>
Tree	reference-bandwidth
Range	1 to 8000000000
Default	400000000
Units	kbps
Configurable	True
Platforms	Supported on all platforms

router-id

Description	Enter the router-id context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> router-id
Tree	router-id
Configurable	True
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> routes-submitted
Tree	routes-submitted
Configurable	False
Platforms	Supported on all platforms

spf

Description	SPF related information
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf
Tree	spf
Configurable	False
Platforms	Supported on all platforms

avg-spf-run-interval *number*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf avg-spf-run-interval <i>number</i>
Tree	avg-spf-run-interval
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf ext-spf-runs
Tree	ext-spf-runs
Configurable	False
Platforms	Supported on all platforms

full-spf-runs

Description	The total number of times that complete SPF has been run on the router since OSPF was last enabled.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf full-spf-runs
Tree	full-spf-runs
Configurable	False
Platforms	Supported on all platforms

incremental-ext-spf-runs

Description	The total number of incremental SPF runs triggered by new or updated external LS-as.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf incremental-ext-spf-runs
Tree	incremental-ext-spf-runs
Configurable	False
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf incremental-inter-spf-runs
Tree	incremental-inter-spf-runs
Configurable	False
Platforms	Supported on all platforms

last-ext-spf

Description	Information about the last external SPF run
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-ext-spf
Tree	last-ext-spf
Configurable	False
Platforms	Supported on all platforms

interval *number*

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-ext-spf interval <i>number</i>
Tree	interval
Range	0 to 2147483647
Units	centiseconds

Configurable	False
Platforms	Supported on all platforms

run-time string

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.
Context	network-instance name string protocols ospf instance name string spf last-ext-spf run-time string
Tree	run-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-full-spf

Description	Information about the last full SPF run
Context	network-instance name string protocols ospf instance name string spf last-full-spf
Tree	last-full-spf
Configurable	False
Platforms	Supported on all platforms

extern-spf-time number

Description	Time it took, in hundredths of seconds, to complete the external LSA calculations.
Context	network-instance name string protocols ospf instance name string spf last-full-spf extern-spf-time number
Tree	extern-spf-time
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

inter-spf-time *number*

Description	Time it took, in hundredths of seconds, to complete the inter-area SPF calculations.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-full-spf inter-spf-time <i>number</i>
Tree	inter-spf-time
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

intra-spf-time *number*

Description	Time it took, in hundredths of seconds, to complete the intra-area SPF calculations.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-full-spf intra-spf-time <i>number</i>
Tree	intra-spf-time
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

rtm-update-time *number*

Description	Time it took, in hundredths of seconds, to complete the RTM updates.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-full-spf rtm-update-time <i>number</i>
Tree	rtm-update-time
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

run-time *string*

Description	The value of last-full-spf-run-time indicates the time at which the system last performed a full dijkstra (SPF) run.
--------------------	--

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-full-spf run-time <i>string</i>
Tree	run-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

total-time *number*

Description	Time it took, in hundredths of seconds, to complete the last SPF run completely.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf last-full-spf total-time <i>number</i>
Tree	total-time
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

max-spf-run-interval *number*

Description	The value of max-spf-run-interval indicates the maximum time, in hundredths of seconds, used to perform a total SPF calculation.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf max-spf-run-interval <i>number</i>
Tree	max-spf-run-interval
Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

min-spf-run-interval *number*

Description	The value of min-spf-run-interval indicates the minimum time, in hundredths of seconds, used to perform a total SPF calculation.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf min-spf-run-interval <i>number</i>
Tree	min-spf-run-interval

Range	0 to 2147483647
Units	centiseconds
Configurable	False
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> spf spf-attempts-failed
Tree	spf-attempts-failed
Configurable	False
Platforms	Supported on all platforms

timers

Description	Enter the timers context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers
Tree	timers
Configurable	True
Platforms	Supported on all platforms

incremental-spf-wait *number*

Description	Delay time before an incremental SPF calculation is started
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers incremental-spf-wait <i>number</i>
Tree	incremental-spf-wait
Range	0 to 1000
Default	1000
Configurable	True
Platforms	Supported on all platforms

lsa-accumulate *number*

Description	Delay time for accumulating multiple LSAs before advertising them to neighbors
--------------------	--

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers lsa-accumulate <i>number</i>
Tree	lsa-accumulate
Range	0 to 1000
Default	1000
Configurable	True
Platforms	Supported on all platforms

lsa-arrival *number*

Description	Minimum delay between receipt of the same LSAs arriving from neighbors
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers lsa-arrival <i>number</i>
Tree	lsa-arrival
Range	0 to 600000
Default	1000
Configurable	True
Platforms	Supported on all platforms

lsa-generate

Description	Enter the lsa-generate context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers lsa-generate
Tree	lsa-generate
Configurable	True
Platforms	Supported on all platforms

lsa-initial-wait *number*

Description	First waiting period between link state advertisements LSA originates
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers lsa-generate lsa-initial-wait <i>number</i>
Tree	lsa-initial-wait
Range	10 to 600000
Default	5000
Units	milliseconds

Configurable	True
Platforms	Supported on all platforms

lsa-second-wait *number*

Description	Hold time between the first and second LSA generation
Context	network-instance name string protocols ospf instance name string timers lsa-generate lsa-second-wait number
Tree	lsa-second-wait
Range	10 to 600000
Default	5000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

max-lsa-wait *number*

Description	Maximum time between two consecutive occurrences of an LSA being generated
Context	network-instance name string protocols ospf instance name string timers lsa-generate max-lsa-wait number
Tree	max-lsa-wait
Range	10 to 600000
Default	5000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

redistribute-delay *number*

Description	Hold down timer for external routes that are redistributed in OSPF
Context	network-instance name string protocols ospf instance name string timers redistribute-delay number
Tree	redistribute-delay
Range	0 to 1000
Default	1000
Configurable	True

Platforms Supported on all platforms

spf-wait

Description Enter the spf-wait context

Context [network-instance name string protocols ospf instance name string timers spf-wait](#)

Tree [spf-wait](#)

Configurable True

Platforms Supported on all platforms

spf-initial-wait *number*

Description Initial SPF calculation delay after a topology change

Context [network-instance name string protocols ospf instance name string timers spf-wait spf-initial-wait number](#)

Tree [spf-initial-wait](#)

Range 10 to 100000

Default 1000

Units milliseconds

Configurable True

Platforms Supported on all platforms

spf-max-wait *number*

Description Maximum interval between two consecutive SPF calculations

Context [network-instance name string protocols ospf instance name string timers spf-wait spf-max-wait number](#)

Tree [spf-max-wait](#)

Range 10 to 120000

Default 10000

Units milliseconds

Configurable True

Platforms Supported on all platforms

spf-second-wait *number*

Description	Hold time between the first and second SPF calculation
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> timers spf-wait spf-second-wait <i>number</i>
Tree	spf-second-wait
Range	10 to 100000
Default	1000
Units	milliseconds
Configurable	True
Platforms	Supported on all platforms

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.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> total-exported-routes
Tree	total-exported-routes
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Enter the trace-options context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace

Description	Tracing parameter flags
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace
Tree	trace

Configurable	True
Platforms	Supported on all platforms

adjacencies

Description	Enable tracing all BGP events.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace adjacencies
Tree	adjacencies
Configurable	True
Platforms	Supported on all platforms

graceful-restart

Description	Enable tracing all graceful-restart events.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace graceful-restart
Tree	graceful-restart
Configurable	True
Platforms	Supported on all platforms

interfaces

Description	Enable tracing all interface events.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace interfaces
Tree	interfaces
Configurable	True
Platforms	Supported on all platforms

lsdb

Description	Trace OSPF LSDB events Only one type can be enabled at a time
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace lsdb
Tree	lsdb
Configurable	True
Platforms	Supported on all platforms

link-state-id *string*

Description	Enter the link-state-id context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace lsdb link-state-id <i>string</i>
Tree	link-state-id
Configurable	True
Platforms	Supported on all platforms

router-id *string*

Description	Enter the router-id context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace lsdb router-id <i>string</i>
Tree	router-id
Configurable	True
Platforms	Supported on all platforms

type *keyword*

Description	Enter the type context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace lsdb type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • all Enable tracing of all LSDB events • router Enable tracing of LSDB router LSA events • network Enable tracing of OSPF LSDB network LSA events • summary Enable tracing of OSPF LSDB summary LSA events • nssa Enable tracing of OSPF LSDB NSSA LSA events • external Enable tracing of OSPF LSDB events for External LSA • opaque

- Enable tracing of OSPF LSDB events involving opaque LSA
 - inter-area-prefix
 - Enable tracing of OSPF LSDB events for inter-area prefixes
 - inter-area-router
 - Enable tracing of OSPF LSDB events for inter-area routers
 - intra-area-prefix
 - Enable tracing of OSPF LSDB events for intra-area prefixes

Configurable True
Platforms Supported on all platforms

misc

Description Enable tracing all Config events.
Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [trace-options trace misc](#)
Tree [misc](#)
Configurable True
Platforms Supported on all platforms

packet

Description Trace OSPF Packet types Only one type can be enabled at a time
Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [trace-options trace packet](#)
Tree [packet](#)
Configurable True
Platforms Supported on all platforms

detail

Description To enable detailed tracing. Includes both received and sent packets.
Context [network-instance name](#) *string* [protocols ospf instance name](#) *string* [trace-options trace packet detail](#)
Tree [detail](#)
Configurable True
Platforms Supported on all platforms

modifier *keyword*

Description	Enter the modifier context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace packet modifier <i>keyword</i>
Tree	modifier
Options	<ul style="list-style-type: none"> • ingress To enable tracing for the packets which are received. • egress To enable tracing for the sent packets. • in-and-egress To enable tracing for both sent and received packets • drop To enable tracing for the sent packets.
Configurable	True
Platforms	Supported on all platforms

type *keyword*

Description	Enter the type context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace packet type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • all Enable tracing of all OSPF packets • hello Enable tracing of OSPF Hello packets • dbdescr Enable tracing of OSPF database Descriptor packets • ls-request Enable tracing of OSPF link-state request packets • ls-update Enable tracing of OSPF link-state update packets • ls-ack Enable tracing of OSPF link-state Ack packets
Configurable	True
Platforms	Supported on all platforms

routes

Description	Enable the routes context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace routes
Tree	routes
Configurable	True
Platforms	Supported on all platforms

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

Description	Enter the dest-address context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace routes dest-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	dest-address
Configurable	True
Platforms	Supported on all platforms

spf

Description	Enable the spf context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace spf
Tree	spf
Configurable	True
Platforms	Supported on all platforms

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

Description	Enter the dest-address context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> trace-options trace spf dest-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	dest-address
Configurable	True
Platforms	Supported on all platforms

version *identityref*

Description	The version that this ospf instance supports.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> version identityref
Tree	version
Options	<ul style="list-style-type: none"> ospf-v2 Version 2 of the OSPF protocol ospf-v3 Version 3 of the OSPF protocol
Configurable	True
Platforms	Supported on all platforms

route-table

Description	Enter the route-table context
Context	network-instance name <i>string</i> route-table
Tree	route-table
Configurable	False
Platforms	Supported on all platforms

ipv4-unicast

Description	The container for the IPv4 unicast routing table of the network instance.
Context	network-instance name <i>string</i> route-table ipv4-unicast
Tree	ipv4-unicast
Configurable	False
Platforms	Supported on all platforms

route [ipv4-prefix](#) *string* [route-type](#) *identityref* [route-owner](#) *string* [id](#) *number*

Description	Enter the route list instance
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i>
Tree	route
Configurable	False
Platforms	Supported on all platforms

ipv4-prefix *string*

Description	The IPv4 prefix associated with the route.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

route-type *identityref*

Description	The type of the IP route
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd IP route added by ARP ND. • bgp Border Gateway Protocol version 4 • bgp-evpn BGP Ethernet VPN (EVPN) • dhcp IP (default) route added by DHCP. • gribi A gRIBI route • host A host route • isis IS-IS • local A directly connected route • linux IP route added by the linux kernel. • ndk1 Route added by an agent application using the NDK • ndk2 Route added by an agent application using the NDK

- ospfv2
OSPFv2
- ospfv3
OSPFv3
- static
Locally configured static route

Configurable	False
Platforms	Supported on all platforms

route-owner *string*

Description	The application name of the owner of the IP route
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

id *number*

Description	An owner-assigned index value that is unique for each of the routes for a given prefix.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

active *boolean*

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.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i> active <i>boolean</i>
Tree	active
Configurable	False
Platforms	Supported on all platforms

fib-programming

Description	Container for state related to the FIB programming of the object
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming
Tree	fib-programming
Configurable	False
Platforms	Supported on all platforms

last-failed-complexes *string*

Description	List of forwarding complexes that reported a failure for the last operation. They appear in the format (slot-number,complex-number).
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming last-failed-complexes <i>string</i>
Tree	last-failed-complexes
Configurable	False
Platforms	Supported on all platforms

last-failed-operation-type *keyword*

Description	The last operation type that failed.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming last-failed-operation-type <i>keyword</i>
Tree	last-failed-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

last-successful-operation-timestamp *string*

Description	The date and time of the last operation to complete successfully. A delete operation is immediately timestamped by FIB manager on the assumption that it will ultimately be successful on all complexes. For other operations the timestamp is generated when the last complex that was expected to respond has responded with a success acknowledgement.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming last-successful-operation-timestamp <i>string</i>
Tree	last-successful-operation-timestamp
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-successful-operation-type *keyword*

Description	The last operation type that completed successfully.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming last-successful-operation-type <i>keyword</i>
Tree	last-successful-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

pending-operation-type *keyword*

Description	The current operation type that is in progress because not all complexes have responded.
--------------------	--

Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i> fib-programming pending-operation-type <i>keyword</i>
Tree	pending-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

gribi-metadata *binary*

Description	Metadata persistently stored with the entry.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i> gribi-metadata <i>binary</i>
Tree	gribi-metadata
String Length	0 to 8
Configurable	False
Platforms	Supported on all platforms

last-app-update *string*

Description	The date and time of the last update of this route by the owning application or protocol.
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i> last-app-update <i>string</i>
Tree	last-app-update
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

metric number

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.
Context	network-instance name string route-table ipv4-unicast route ipv4-prefix string route-type identityref route-owner string id number metric number
Tree	metric
Configurable	False
Platforms	Supported on all platforms

next-hop-group reference

Description	The next-hop-group indirection object used by this route.
Context	network-instance name string route-table ipv4-unicast route ipv4-prefix string route-type identityref route-owner string id number next-hop-group reference
Tree	next-hop-group
Reference	network-instance name string route-table next-hop-group index number
Configurable	False
Platforms	Supported on all platforms

next-hop-group-network-instance reference

Description	The network instance where the next-hop-group can be found. If unspecified, the next hop group is in the local network instance.
Context	network-instance name string route-table ipv4-unicast route ipv4-prefix string route-type identityref route-owner string id number next-hop-group-network-instance reference
Tree	next-hop-group-network-instance
Reference	network-instance name string
Configurable	False
Platforms	Supported on all platforms

preference number

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.
Context	network-instance name string route-table ipv4-unicast route ipv4-prefix string route-type identityref route-owner string id number preference number

Tree	preference
Configurable	False
Platforms	Supported on all platforms

resilient-hash *boolean*

Description	Set to true if the route is covered by a resilient-hash-prefix entry
Context	network-instance name <i>string</i> route-table ipv4-unicast route ipv4-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number resilient-hash <i>boolean</i>
Tree	resilient-hash
Configurable	False
Platforms	Supported on all platforms

route-summary

Description	Route summary information
Context	network-instance name <i>string</i> route-table ipv4-unicast route-summary
Tree	route-summary
Configurable	False
Platforms	Supported on all platforms

route-type [ip-route-type-name](#) *identityref*

Description	Enter the route-type list instance
Context	network-instance name <i>string</i> route-table ipv4-unicast route-summary route-type ip-route-type-name <i>identityref</i>
Tree	route-type
Configurable	False
Platforms	Supported on all platforms

ip-route-type-name *identityref*

Description	IP route type
Context	network-instance name <i>string</i> route-table ipv4-unicast route-summary route-type ip-route-type-name <i>identityref</i>
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd

IP route added by ARP ND.

- `bgp`
Border Gateway Protocol version 4
- `bgp-evpn`
BGP Ethernet VPN (EVPN)
- `dhcp`
IP (default) route added by DHCP.
- `gribi`
A gRIBI route
- `host`
A host route
- `isis`
IS-IS
- `local`
A directly connected route
- `linux`
IP route added by the linux kernel.
- `ndk1`
Route added by an agent application using the NDK
- `ndk2`
Route added by an agent application using the NDK
- `ospfv2`
OSPFv2
- `ospfv3`
OSPFv3
- `static`
Locally configured static route

Configurable	False
Platforms	Supported on all platforms

active-routes *number*

Description	Total number of prefixes associated with this route type that were submitted to fib-mgr and that fib-mgr successfully installed as active routes
Context	network-instance name <i>string</i> route-table ipv4-unicast route-summary route-type ip-route-type-name <i>identityref</i> active-routes <i>number</i>
Tree	active-routes

Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> route-table ipv4-unicast statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-routes *number*

Description	The total number of prefixes, belonging to this address family, with an active route in the FIB.
Context	network-instance name <i>string</i> route-table ipv4-unicast statistics active-routes <i>number</i>
Tree	active-routes
Configurable	False
Platforms	Supported on all platforms

active-routes-with-ecmp *number*

Description	The total number of prefixes, belonging to this address family, that have an active route in the FIB with multiple ECMP next-hops.
Context	network-instance name <i>string</i> route-table ipv4-unicast statistics active-routes-with-ecmp <i>number</i>
Tree	active-routes-with-ecmp
Configurable	False
Platforms	Supported on all platforms

fib-failed-routes *number*

Description	The total number of prefixes, belonging to this address family, that were not installed successfully because datapath resources were unavailable.
Context	network-instance name <i>string</i> route-table ipv4-unicast statistics fib-failed-routes <i>number</i>
Tree	fib-failed-routes

Configurable	False
Platforms	Supported on all platforms

resilient-hash-routes *number*

Description	The total number of prefixes, belonging to this address family, with an active route in the FIB that have resilient hash support.
Context	network-instance name <i>string</i> route-table ipv4-unicast statistics resilient-hash-routes <i>number</i>
Tree	resilient-hash-routes
Configurable	False
Platforms	Supported on all platforms

total-routes *number*

Description	The total number of routes, active and inactive, belonging to this address family, that are present in the routing table.
Context	network-instance name <i>string</i> route-table ipv4-unicast statistics total-routes <i>number</i>
Tree	total-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

ipv6-unicast

Description	The container for the IPv6 unicast routing table of the network instance.
Context	network-instance name <i>string</i> route-table ipv6-unicast
Tree	ipv6-unicast
Configurable	False
Platforms	Supported on all platforms

route [ipv6-prefix](#) *string* [route-type](#) [identityref](#) [route-owner](#) *string* [id](#) *number*

Description	Enter the route list instance
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Tree	route

Configurable	False
Platforms	Supported on all platforms

ipv6-prefix *string*

Description	The IPv6 prefix associated with the route.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string id number</i>
Configurable	False
Platforms	Supported on all platforms

route-type *identityref*

Description	The type of the IP route
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string id number</i>
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd IP route added by ARP ND. • bgp Border Gateway Protocol version 4 • bgp-evpn BGP Ethernet VPN (EVPN) • dhcp IP (default) route added by DHCP. • gribi A gRIBI route • host A host route • isis IS-IS • local A directly connected route • linux IP route added by the linux kernel. • ndk1 Route added by an agent application using the NDK

- ndk2
Route added by an agent application using the NDK
- ospfv2
OSPFv2
- ospfv3
OSPFv3
- static
Locally configured static route

Configurable	False
Platforms	Supported on all platforms

route-owner *string*

Description	The application name of the owner of the IP route
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

id *number*

Description	An owner-assigned index value that is unique for each of the routes for a given prefix.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

active *boolean*

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.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i> active <i>boolean</i>
Tree	active
Configurable	False
Platforms	Supported on all platforms

fib-programming

Description	Container for state related to the FIB programming of the object
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i> fib-programming
Tree	fib-programming
Configurable	False
Platforms	Supported on all platforms

last-failed-complexes *string*

Description	List of forwarding complexes that reported a failure for the last operation. They appear in the format (slot-number,complex-number).
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i> fib-programming last-failed-complexes <i>string</i>
Tree	last-failed-complexes
Configurable	False
Platforms	Supported on all platforms

last-failed-operation-type *keyword*

Description	The last operation type that failed.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id <i>number</i> fib-programming last-failed-operation-type <i>keyword</i>
Tree	last-failed-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

last-successful-operation-timestamp *string*

Description	The date and time of the last operation to complete successfully. A delete operation is immediately timestamped by FIB manager on the assumption that it will ultimately be successful on all complexes. For other operations the timestamp is generated when the last complex that was expected to respond has responded with a success acknowledgement.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming last-successful-operation-timestamp <i>string</i>
Tree	last-successful-operation-timestamp
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-successful-operation-type *keyword*

Description	The last operation type that completed successfully.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number fib-programming last-successful-operation-type <i>keyword</i>
Tree	last-successful-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

pending-operation-type *keyword*

Description	The current operation type that is in progress because not all complexes have responded.
--------------------	--

Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i> fib-programming pending-operation-type <i>keyword</i>
Tree	pending-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

gribi-metadata *binary*

Description	Metadata persistently stored with the entry.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i> gribi-metadata <i>binary</i>
Tree	gribi-metadata
String Length	0 to 8
Configurable	False
Platforms	Supported on all platforms

last-app-update *string*

Description	The date and time of the last update of this route by the owning application or protocol.
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type <i>identityref</i> route-owner <i>string</i> id <i>number</i> last-app-update <i>string</i>
Tree	last-app-update
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

metric number

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.
Context	network-instance name string route-table ipv6-unicast route ipv6-prefix string route-type identityref route-owner string id number metric number
Tree	metric
Configurable	False
Platforms	Supported on all platforms

next-hop-group reference

Description	The next-hop-group indirection object used by this route.
Context	network-instance name string route-table ipv6-unicast route ipv6-prefix string route-type identityref route-owner string id number next-hop-group reference
Tree	next-hop-group
Reference	network-instance name string route-table next-hop-group index number
Configurable	False
Platforms	Supported on all platforms

next-hop-group-network-instance reference

Description	The network instance where the next-hop-group can be found. If unspecified, the next hop group is in the local network instance.
Context	network-instance name string route-table ipv6-unicast route ipv6-prefix string route-type identityref route-owner string id number next-hop-group-network-instance reference
Tree	next-hop-group-network-instance
Reference	network-instance name string
Configurable	False
Platforms	Supported on all platforms

preference number

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.
Context	network-instance name string route-table ipv6-unicast route ipv6-prefix string route-type identityref route-owner string id number preference number

Tree	preference
Configurable	False
Platforms	Supported on all platforms

resilient-hash *boolean*

Description	Set to true if the route is covered by a resilient-hash-prefix entry
Context	network-instance name <i>string</i> route-table ipv6-unicast route ipv6-prefix <i>string</i> route-type identityref route-owner <i>string</i> id number resilient-hash <i>boolean</i>
Tree	resilient-hash
Configurable	False
Platforms	Supported on all platforms

route-summary

Description	Route summary information
Context	network-instance name <i>string</i> route-table ipv6-unicast route-summary
Tree	route-summary
Configurable	False
Platforms	Supported on all platforms

route-type [ip-route-type-name](#) *identityref*

Description	Enter the route-type list instance
Context	network-instance name <i>string</i> route-table ipv6-unicast route-summary route-type ip-route-type-name <i>identityref</i>
Tree	route-type
Configurable	False
Platforms	Supported on all platforms

ip-route-type-name *identityref*

Description	IP route type
Context	network-instance name <i>string</i> route-table ipv6-unicast route-summary route-type ip-route-type-name <i>identityref</i>
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd

IP route added by ARP ND.

- `bgp`
Border Gateway Protocol version 4
- `bgp-evpn`
BGP Ethernet VPN (EVPN)
- `dhcp`
IP (default) route added by DHCP.
- `gribi`
A gRIBI route
- `host`
A host route
- `isis`
IS-IS
- `local`
A directly connected route
- `linux`
IP route added by the linux kernel.
- `ndk1`
Route added by an agent application using the NDK
- `ndk2`
Route added by an agent application using the NDK
- `ospfv2`
OSPFv2
- `ospfv3`
OSPFv3
- `static`
Locally configured static route

Configurable	False
Platforms	Supported on all platforms

active-routes *number*

Description	Total number of prefixes associated with this route type that were submitted to fib-mgr and that fib-mgr successfully installed as active routes
Context	network-instance name <i>string</i> route-table ipv6-unicast route-summary route-type ip-route-type-name <i>identityref</i> active-routes <i>number</i>
Tree	active-routes

Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> route-table ipv6-unicast statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-routes *number*

Description	The total number of prefixes, belonging to this address family, with an active route in the FIB.
Context	network-instance name <i>string</i> route-table ipv6-unicast statistics active-routes <i>number</i>
Tree	active-routes
Configurable	False
Platforms	Supported on all platforms

active-routes-with-ecmp *number*

Description	The total number of prefixes, belonging to this address family, that have an active route in the FIB with multiple ECMP next-hops.
Context	network-instance name <i>string</i> route-table ipv6-unicast statistics active-routes-with-ecmp <i>number</i>
Tree	active-routes-with-ecmp
Configurable	False
Platforms	Supported on all platforms

fib-failed-routes *number*

Description	The total number of prefixes, belonging to this address family, that were not installed successfully because datapath resources were unavailable.
Context	network-instance name <i>string</i> route-table ipv6-unicast statistics fib-failed-routes <i>number</i>
Tree	fib-failed-routes

Configurable	False
Platforms	Supported on all platforms

resilient-hash-routes *number*

Description	The total number of prefixes, belonging to this address family, with an active route in the FIB that have resilient hash support.
Context	network-instance name <i>string</i> route-table ipv6-unicast statistics resilient-hash-routes <i>number</i>
Tree	resilient-hash-routes
Configurable	False
Platforms	Supported on all platforms

total-routes *number*

Description	The total number of routes, active and inactive, belonging to this address family, that are present in the routing table.
Context	network-instance name <i>string</i> route-table ipv6-unicast statistics total-routes <i>number</i>
Tree	total-routes
Default	0
Configurable	False
Platforms	Supported on all platforms

mpls

Description	The container for the MPLS routing table of the network instance.
Context	network-instance name <i>string</i> route-table mpls
Tree	mpls
Configurable	False
Platforms	Supported on all platforms

label-entry [label-value](#) *number*

Description	Enter the label-entry list instance
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i>
Tree	label-entry

Configurable	False
Platforms	Supported on all platforms

label-value *number*

Description	The MPLS label value
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i>
Range	16 to 1048575
Configurable	False
Platforms	Supported on all platforms

entry-type *identityref*

Description	The entry type of the MPLS FIB entry.
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i> entry-type <i>identityref</i>
Tree	entry-type
Options	<ul style="list-style-type: none"> • ldp Label distribution protocol • sr-mpls Segment routing using MPLS dataplane, programmed by segment routing manager. • sr-policy-mpls Tunnels setup using SR-POLICY. • static-mpls Locally configured static MPLS route.
Configurable	False
Platforms	Supported on all platforms

last-app-update *string*

Description	The date and time of the last update of this MPLS label entry by the owning application or protocol.
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i> last-app-update <i>string</i>
Tree	last-app-update
String Length	20 to 32

Configurable	False
Platforms	Supported on all platforms

next-hop-group *reference*

Description	The next-hop-group indirection object used by this route. Applicable only if the operation is SWAP.
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i> next-hop-group reference
Tree	next-hop-group
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

next-network-instance *reference*

Description	If this ILM entry is for a pop label, and this label is at the bottom of the stack, the next forwarding lookup will be done in the referenced network-instance
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i> next-network-instance reference
Tree	next-network-instance
Reference	network-instance name <i>string</i>
Configurable	False
Platforms	Supported on all platforms

operation *keyword*

Description	The forwarding operation associated with the MPLS label entry.
Context	network-instance name <i>string</i> route-table mpls label-entry label-value <i>number</i> operation keyword
Tree	operation
Options	<ul style="list-style-type: none"> • pop • swap
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> route-table mpls statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-entries *number*

Description	The total number of MPLS entries that are active in the FIB.
Context	network-instance name <i>string</i> route-table mpls statistics active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

next-hop [index](#) *number*

Description	Enter the next-hop list instance
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i>
Tree	next-hop
Configurable	False
Platforms	Supported on all platforms

index *number*

Description	A system-wide unique identifier of a next-hop object (system allocated).
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

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

Description	The next-hop IP address. Only populated when the next-hop type is indirect or tunnel or static-mpls. For a VXLAN tunnel this is the destination VTEP address.
--------------------	--

Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> ip-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	ip-address
Configurable	False
Platforms	Supported on all platforms

mpls

Description	Enter the mpls context
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> mpls
Tree	mpls
Configurable	False
Platforms	Supported on all platforms

pushed-mpls-label-stack (*number* | *keyword*)

Description	The list of MPLS labels to push onto the packet when forwarding to this particular next-hop.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> mpls pushed-mpls-label-stack (<i>number</i> <i>keyword</i>)
Tree	pushed-mpls-label-stack
Range	16 to 1048575
Options	<ul style="list-style-type: none"> • IPV4_EXPLICIT_NULL • IPV6_EXPLICIT_NULL • IMPLICIT_NULL
Configurable	False
Platforms	Supported on all platforms
Max. Elements	1

network-instance *reference*

Description	Indicates that the next-hop is another network instance. If this is specified but an IP address or interface is not provided, the meaning is that a new IP lookup should occur in the other network instance.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> network-instance <i>reference</i>
Tree	network-instance
Reference	network-instance name <i>string</i>

Configurable	False
Platforms	Supported on all platforms

programmed-index *number*

Description	The index assigned to the next-hop by the gRIBI client
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> programmed-index <i>number</i>
Tree	programmed-index
Configurable	False
Platforms	Supported on all platforms

resolving-route

Description	Enter the resolving-route context
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route
Tree	resolving-route
Configurable	False
Platforms	Supported on all platforms

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	The prefix of the resolving route.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Tree	ip-prefix
Configurable	False
Platforms	Supported on all platforms

route-owner *string*

Description	The application name of the owner of the resolving route.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route route-owner <i>string</i>
Tree	route-owner
Configurable	False
Platforms	Supported on all platforms

route-type *identityref*

Description	The type of the resolving route.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> resolving-route route-type <i>identityref</i>
Tree	route-type
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd IP route added by ARP ND. • bgp Border Gateway Protocol version 4 • bgp-evpn BGP Ethernet VPN (EVPN) • dhcp IP (default) route added by DHCP. • gribi A gRIBI route • host A host route • isis IS-IS • local A directly connected route • linux IP route added by the linux kernel. • ndk1 Route added by an agent application using the NDK • ndk2 Route added by an agent application using the NDK • ospfv2 OSPFv2 • ospfv3 OSPFv3 • static Locally configured static route
Configurable	False

Platforms Supported on all platforms

resolving-tunnel

Description Enter the resolving-tunnel context

Context [network-instance name](#) *string* [route-table](#) [next-hop index](#) *number* [resolving-tunnel](#)

Tree [resolving-tunnel](#)

Configurable False

Platforms Supported on all platforms

ip-prefix (*ipv4-prefix* | *ipv6-prefix*)

Description The prefix of the resolving tunnel.

Context [network-instance name](#) *string* [route-table](#) [next-hop index](#) *number* [resolving-tunnel](#) [ip-prefix](#) (*ipv4-prefix* | *ipv6-prefix*)

Tree [ip-prefix](#)

Configurable False

Platforms Supported on all platforms

tunnel-owner *string*

Description The application name of the owner of the resolving tunnel.

Context [network-instance name](#) *string* [route-table](#) [next-hop index](#) *number* [resolving-tunnel](#) [tunnel-owner](#) *string*

Tree [tunnel-owner](#)

Configurable False

Platforms Supported on all platforms

tunnel-type *identityref*

Description The type of the tunnel.

Context [network-instance name](#) *string* [route-table](#) [next-hop index](#) *number* [resolving-tunnel](#) [tunnel-type](#) *identityref*

Tree [tunnel-type](#)

Options

- sr-isis
Segment routing using MPLS dataplane, programmed by IS-IS
- sr-ospfv2

- Segment routing using MPLS dataplane, programmed by OSPFv2
- sr-ospfv3
- Segment routing using MPLS dataplane, programmed by OSPFv3
- vxlan
- Tunnels based on VXLAN encapsulation

Configurable	False
Platforms	Supported on all platforms

subinterface *reference*

Description	The next-hop interface. Only populated when the next-hop type is direct.
Context	network-instance name <i>string</i> route-table <i>string</i> next-hop index <i>number</i> subinterface <i>reference</i>
Tree	subinterface
Reference	interface name <i>string</i> subinterface index <i>number</i> name <i>string</i>
Configurable	False
Platforms	Supported on all platforms

type *identityref*

Description	The next-hop type used by the datapath.
Context	network-instance name <i>string</i> route-table <i>string</i> next-hop index <i>number</i> type <i>identityref</i>
Tree	type
Options	<ul style="list-style-type: none"> • extract <p>Next-hop will cause matching packets to be delivered to the CPM.</p> • direct <p>Next-hop was resolved by a local route - i.e. it is an address on a connected subnet.</p> • discard <p>Next-hop will cause matching packets to be dropped without ICMP generation.</p> • reject <p>Next-hop will cause matching packets to be dropped with ICMP generation.</p> • indirect <p>Next-hop was resolved by a non-local route - i.e. it is not an address on a connected subnet.</p>

- `mpls`
An MPLS label will be pushed when forwarding to this next-hop.
- `tunnel`
Next-hop is a tunnel.
- `broadcast`
Next-hop will cause matching subnet-broadcast packets to be delivered to the control plane.

Configurable	False
Platforms	Supported on all platforms

vxlan

Description	Enter the vxlan context
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> vxlan
Tree	vxlan
Configurable	False
Platforms	Supported on all platforms

destination-mac *string*

Description	VXLAN inner ethernet destination mac-address.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> vxlan destination-mac <i>string</i>
Tree	destination-mac
Configurable	False
Platforms	Supported on all platforms

source-mac *string*

Description	VXLAN inner ethernet source mac-address.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> vxlan source-mac <i>string</i>
Tree	source-mac
Configurable	False
Platforms	Supported on all platforms

vni number

Description	VXLAN Network Identifier of the destination.
Context	network-instance name <i>string</i> route-table next-hop index <i>number</i> vxlan vni number
Tree	vni
Range	1 to 16777215
Configurable	False
Platforms	Supported on all platforms

next-hop-group index number

Description	Enter the next-hop-group list instance
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Tree	next-hop-group
Configurable	False
Platforms	Supported on all platforms

index number

Description	A system-wide unique identifier of a next-hop-group indirection object (system allocated).
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

backup-next-hop-group reference

Description	The backup next-hop-group for the current group. When all entries within the next-hop group become unusable, the backup next-hop group is used if specified.
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> backup-next-hop-group reference
Tree	backup-next-hop-group
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

fib-programming

Description	Container for state related to the FIB programming of the object
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> fib-programming
Tree	fib-programming
Configurable	False
Platforms	Supported on all platforms

last-failed-complexes *string*

Description	List of forwarding complexes that reported a failure for the last operation. They appear in the format (slot-number,complex-number).
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> fib-programming last-failed-complexes <i>string</i>
Tree	last-failed-complexes
Configurable	False
Platforms	Supported on all platforms

last-failed-operation-type *keyword*

Description	The last operation type that failed.
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> fib-programming last-failed-operation-type <i>keyword</i>
Tree	last-failed-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

last-successful-operation-timestamp *string*

Description	The date and time of the last operation to complete successfully. A delete operation is immediately timestamped by FIB manager on the assumption that it will ultimately be successful on all complexes. For other operations the timestamp is generated when the last complex that was expected to respond has responded with a success acknowledgement.
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> fib-programming last-successful-operation-timestamp <i>string</i>
Tree	last-successful-operation-timestamp
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-successful-operation-type *keyword*

Description	The last operation type that completed successfully.
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> fib-programming last-successful-operation-type <i>keyword</i>
Tree	last-successful-operation-type
Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

pending-operation-type *keyword*

Description	The current operation type that is in progress because not all complexes have responded.
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> fib-programming pending-operation-type <i>keyword</i>
Tree	pending-operation-type

Options	<ul style="list-style-type: none"> • add The current or last operation was an attempt to create a new entry. • delete The current or last operation was an attempt to delete an existing entry. • modify The current or last operation was an attempt to modify an existing entry. • none There was no prior operation for this entry or there is no current operation that is in process
Configurable	False
Platforms	Supported on all platforms

next-hop id number

Description	Enter the next-hop list instance
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
Configurable	False
Platforms	Supported on all platforms

id number

Description	A unique identifier of a next-hop member (system allocated).
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> next-hop id <i>number</i>
Range	0 to 1023
Configurable	False
Platforms	Supported on all platforms

next-hop reference

Description	Enter the next-hop context
Context	network-instance name <i>string</i> route-table next-hop-group index <i>number</i> next-hop id <i>number</i> next-hop reference
Tree	next-hop
Reference	network-instance name <i>string</i> route-table next-hop index <i>number</i>
Configurable	False

Platforms Supported on all platforms

resolved *keyword*

Description Set to true when the next-hop was resolved. This reads not-applicable for resolve=false next-hops.

Context [network-instance name](#) *string* [route-table](#) [next-hop-group](#) [index](#) *number* [next-hop id](#) *number* **resolved** *keyword*

Tree [resolved](#)

Options

- true
- false
- not-applicable

Configurable False

Platforms Supported on all platforms

weight *number*

Description The actual weight applied to the next-hop within the group. This may differ from the configured weight because the datapath normalizes the weight and expresses it as a percentage. Traffic is balanced across the next-hops within the group in the proportion of weight.

If there are two next-hops in the NHG, N1 with a weight of W1 and N2 with a weight of W2 such that $W1 = n \times W2$, then N1 should ideally have n times as many hash buckets as N2. However, since fractional hash buckets do not exist and there are only 128 hash buckets in total for a given level of ECMP, the actual weight of a next-hop may differ from the ratio expected by taking the configured weight of the next-hop and dividing it by the sum of all the configured weights.

Context [network-instance name](#) *string* [route-table](#) [next-hop-group](#) [index](#) *number* [next-hop id](#) *number* **weight** *number*

Tree [weight](#)

Range 0 to 100

Configurable False

Platforms Supported on all platforms

programmed-index *number*

Description The index assigned to the next-hop-group by the gRIBI client

Context [network-instance name](#) *string* [route-table](#) [next-hop-group](#) [index](#) *number* **programmed-index** *number*

Tree	programmed-index
Configurable	False
Platforms	Supported on all platforms

router-id *string*

Description	A identifier for the local network instance - typically used within associated routing protocols or signalling routing information in another network instance
Context	network-instance name <i>string</i> router-id <i>string</i>
Tree	router-id
Configurable	True
Platforms	Supported on all platforms

segment-routing

Description	Container with segment routing configuration options
Context	network-instance name <i>string</i> segment-routing
Tree	segment-routing
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

mpls

Description	Adding this container activates datapath support for SR-MPLS
Context	network-instance name <i>string</i> segment-routing mpls
Tree	mpls
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

sid-database

Description	Database of all known prefix SIDs, local and remote.
Context	network-instance name <i>string</i> segment-routing mpls sid-database
Tree	sid-database
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

prefix-sid *prefix (ipv4-prefix | ipv6-prefix) sid-label-value number protocol keyword protocol-instance number protocol-multi-topology number algorithm number*

Description	List of prefix SIDs
Context	network-instance name string segment-routing mpls sid-database prefix-sid prefix (ipv4-prefix ipv6-prefix) sid-label-value number protocol keyword protocol-instance number protocol-multi-topology number algorithm number
Tree	prefix-sid
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

prefix *(ipv4-prefix | ipv6-prefix)*

Description	The IPv4 or IPv6 prefix associated with the SID.
Context	network-instance name string segment-routing mpls sid-database prefix-sid prefix (ipv4-prefix ipv6-prefix) sid-label-value number protocol keyword protocol-instance number protocol-multi-topology number algorithm number
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sid-label-value *number*

Description	The MPLS label value associated with the SID.
Context	network-instance name string segment-routing mpls sid-database prefix-sid prefix (ipv4-prefix ipv6-prefix) sid-label-value number protocol keyword protocol-instance number protocol-multi-topology number algorithm number
Range	16 to 1048575
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

protocol *keyword*

Description	The protocol that provided the prefix SID
Context	network-instance name string segment-routing mpls sid-database prefix-sid prefix (ipv4-prefix ipv6-prefix) sid-label-value number protocol keyword protocol-instance number protocol-multi-topology number algorithm number
Options	<ul style="list-style-type: none"> isis direct
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

protocol-instance *number*

Description The instance ID that provided the prefix SID

Context [network-instance name](#) *string* [segment-routing mpls sid-database prefix-sid prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [sid-label-value](#) *number* [protocol keyword](#) [protocol-instance number](#) [protocol-multi-topology number](#) [algorithm number](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

protocol-multi-topology *number*

Description The multi-topology ID that provided the prefix SID

Context [network-instance name](#) *string* [segment-routing mpls sid-database prefix-sid prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [sid-label-value](#) *number* [protocol keyword](#) [protocol-instance number](#) [protocol-multi-topology number](#) [algorithm number](#)

Range 0 to 4095

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

algorithm *number*

Description Contains the identifier of the algorithm the router uses to compute the reachability of the prefix to which the Prefix-SID is associated

Context [network-instance name](#) *string* [segment-routing mpls sid-database prefix-sid prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [sid-label-value](#) *number* [protocol keyword](#) [protocol-instance number](#) [protocol-multi-topology number](#) [algorithm number](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

active *boolean*

Description When false, the prefix SID is inactive.

It could be inactive because it is involved in a prefix or SID conflict that occurred between different protocol-instance. It could also be inactive because datapath programming failed.

Context [network-instance name](#) *string* [segment-routing mpls sid-database prefix-sid prefix](#) (*ipv4-prefix* | *ipv6-prefix*) [sid-label-value](#) *number* [protocol keyword](#)

[protocol-instance](#) *number* [protocol-multi-topology](#) *number* [algorithm](#) *number*
[active](#) *boolean*

Tree	active
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

prefix-conflict *boolean*

Description	Reads true when the prefix SID entry is involved in a prefix conflict that has occurred between protocols. This occurs when there are multiple entries in the SID database for the same prefix. All the conflicting entries become inactive except for the one with the smallest sid-index.
Context	network-instance <i>name</i> <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> protocol <i>keyword</i> protocol-instance <i>number</i> protocol-multi-topology <i>number</i> algorithm <i>number</i> prefix-conflict <i>boolean</i>
Tree	prefix-conflict
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

sid-conflict *boolean*

Description	Reads true when the prefix SID entry is involved in a SID conflict that has occurred between protocols (after first removing inter-protocol prefix conflict entries). All entries involved in a SID conflict that do not have the absolute lowest 'preference' value become inactive. In the SRL implementation local-prefix-sid entries are considered to have a lower numerical preference than remote prefix-sid entries. If there are still SID conflicts then all the remaining conflicting entries become inactive except for the one with the smallest sid-index.
Context	network-instance <i>name</i> <i>string</i> segment-routing mpls sid-database prefix-sid prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) sid-label-value <i>number</i> protocol <i>keyword</i> protocol-instance <i>number</i> protocol-multi-topology <i>number</i> algorithm <i>number</i> sid-conflict <i>boolean</i>
Tree	sid-conflict
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

static-routes

Description	Enable the static-routes context
Context	network-instance <i>name</i> <i>string</i> static-routes

Tree	static-routes
Configurable	True
Platforms	Supported on all platforms

route prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the route list instance
Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Tree	route
Configurable	True
Platforms	Supported on all platforms
Max. Elements	16384

prefix (*ipv4-prefix* | *ipv6-prefix*)

Description	Enter the prefix context
Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>)
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Used to disable the static route.
Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

installed *boolean*

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

Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) installed <i>boolean</i>
Tree	installed
Configurable	False
Platforms	Supported on all platforms

metric number

Description	IGP metric of the static route.
Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) metric <i>number</i>
Tree	metric
Default	1
Configurable	True
Platforms	Supported on all platforms

next-hop-group reference

Description	Enter the next-hop-group context
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
Reference	network-instance name <i>string</i> next-hop-groups group name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

preference number

Description	Route preference with lower values indicating a higher degree of preference.
Context	network-instance name <i>string</i> static-routes route prefix (<i>ipv4-prefix ipv6-prefix</i>) preference <i>number</i>
Tree	preference
Range	0 to 255
Default	5
Configurable	True
Platforms	Supported on all platforms

system-ipv4-address

Description	Container for displaying information about the system IPv4 address of the default network-instance
Context	network-instance name <i>string</i> system-ipv4-address
Tree	system-ipv4-address
Configurable	False
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The reason why the default network instance does not have a system IPv4 address
Context	network-instance name <i>string</i> system-ipv4-address oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • system-interface-not-bound • system-interface-has-no-ipv4-address
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of the system IPv4 address binding
Context	network-instance name <i>string</i> system-ipv4-address oper-state <i>keyword</i>
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

system-ipv6-address

Description	Container for displaying information about the system IPv6 address of the default network-instance
Context	network-instance name <i>string</i> system-ipv6-address
Tree	system-ipv6-address
Configurable	False
Platforms	Supported on all platforms

oper-down-reason *keyword*

Description	The reason why the default network instance does not have a system IPv6 address
--------------------	---

Context	network-instance name <i>string</i> system-ipv6-address oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • system-interface-not-bound • system-interface-has-no-ipv6-address
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of the system IPv6 address binding
Context	network-instance name <i>string</i> system-ipv6-address oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting

Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.

- waiting

Component or process is currently waiting

Component or process is currently waiting This state can be set by event handler when the `reinvoke-with-delay` action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

tcp

Description	State for TCP connections that have been established or could be established using the route tables of this network instance.
Context	network-instance name <i>string</i> tcp
Tree	tcp
Configurable	False
Platforms	Supported on all platforms

connection [local-address](#) (*ipv4-address* | *ipv6-address*) [local-port](#) *number* [remote-address](#) (*ipv4-address* | *ipv6-address*) [remote-port](#) *number*

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.
Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address</i> <i>ipv6-address</i>) remote-port <i>number</i>
Tree	connection
Configurable	False
Platforms	Supported on all platforms

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

Description	The local IP address for this TCP connection.
--------------------	---

Context	network-instance name <i>string</i> tcp connection local-address (ipv4-address ipv6-address) local-port <i>number</i> remote-address (ipv4-address ipv6-address) remote-port <i>number</i>
Configurable	False
Platforms	Supported on all platforms

local-port *number*

Description	The local port number for this TCP connection.
Context	network-instance name <i>string</i> tcp connection local-address (ipv4-address ipv6-address) local-port <i>number</i> remote-address (ipv4-address ipv6-address) remote-port <i>number</i>
Range	0 to 65535
Configurable	False
Platforms	Supported on all platforms

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

Description	The remote IP address for this TCP connection.
Context	network-instance name <i>string</i> tcp connection local-address (ipv4-address ipv6-address) local-port <i>number</i> remote-address (ipv4-address ipv6-address) remote-port <i>number</i>
Configurable	False
Platforms	Supported on all platforms

remote-port *number*

Description	The remote port number for this TCP connection.
Context	network-instance name <i>string</i> tcp connection local-address (ipv4-address ipv6-address) local-port <i>number</i> remote-address (ipv4-address ipv6-address) remote-port <i>number</i>
Range	0 to 65535
Configurable	False
Platforms	Supported on all platforms

process-id *number*

Description	The process ID of the application that owns the socket.
--------------------	---

Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address</i> <i>ipv6-address</i>) remote-port <i>number</i> process-id <i>number</i>
Tree	process-id
Configurable	False
Platforms	Supported on all platforms

session-state *keyword*

Description	The state of this TCP connection.
Context	network-instance name <i>string</i> tcp connection local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i> remote-address (<i>ipv4-address</i> <i>ipv6-address</i>) remote-port <i>number</i> session-state <i>keyword</i>
Tree	session-state
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
Platforms	Supported on all platforms

listening-application [local-address](#) (*ipv4-address* | *ipv6-address*) [local-port](#) *number*

Description	List of applications that are listening on a particular TCP port bound to the network-instance.
Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i>
Tree	listening-application
Configurable	False
Platforms	Supported on all platforms

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

Description	The local IP address accepted by the application. An all-zeroes value for the <i>ipv4-address</i> means that any IPv4 address is accepted. An all-zeroes value for the <i>ipv6-address</i> means that any IPv6 address is accepted.
Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i>
Configurable	False
Platforms	Supported on all platforms

local-port *number*

Description	The local port number accepted by the application.
Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i>
Range	0 to 65535
Configurable	False
Platforms	Supported on all platforms

process-id *number*

Description	The process ID of the application that owns the socket.
Context	network-instance name <i>string</i> tcp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i> process-id <i>number</i>
Tree	process-id
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> tcp statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-opens *number*

Description	The total number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Context	network-instance name <i>string</i> tcp statistics active-opens <i>number</i>
Tree	active-opens
Default	0
Configurable	False
Platforms	Supported on all platforms

attempt-fails *number*

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.
Context	network-instance name <i>string</i> tcp statistics attempt-fails <i>number</i>
Tree	attempt-fails
Default	0
Configurable	False
Platforms	Supported on all platforms

established-resets *number*

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.
Context	network-instance name <i>string</i> tcp statistics established-resets <i>number</i>
Tree	established-resets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-checksum-errors *number*

Description	The total number of segments that are received as bad TCP checksum errors.
Context	network-instance name <i>string</i> tcp statistics in-checksum-errors <i>number</i>
Tree	in-checksum-errors

Default	0
Configurable	False
Platforms	Supported on all platforms

in-error-segments *number*

Description	The total number of segments received in error (e.g., bad TCP checksums).
Context	network-instance name <i>string</i> tcp statistics in-error-segments <i>number</i>
Tree	in-error-segments
Default	0
Configurable	False
Platforms	Supported on all platforms

in-segments *number*

Description	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Context	network-instance name <i>string</i> tcp statistics in-segments <i>number</i>
Tree	in-segments
Default	0
Configurable	False
Platforms	Supported on all platforms

out-rst-segments *number*

Description	The total number of TCP segments sent containing the RST flag.
Context	network-instance name <i>string</i> tcp statistics out-rst-segments <i>number</i>
Tree	out-rst-segments
Default	0
Configurable	False
Platforms	Supported on all platforms

out-segments *number*

Description	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Context	network-instance name <i>string</i> tcp statistics out-segments <i>number</i>

Tree	out-segments
Default	0
Configurable	False
Platforms	Supported on all platforms

passive-opens *number*

Description	The total number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Context	network-instance name <i>string</i> tcp statistics passive-opens <i>number</i>
Tree	passive-opens
Default	0
Configurable	False
Platforms	Supported on all platforms

retransmitted-segments *number*

Description	The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Context	network-instance name <i>string</i> tcp statistics retransmitted-segments <i>number</i>
Tree	retransmitted-segments
Default	0
Configurable	False
Platforms	Supported on all platforms

tunnel-table

Description	Enter the tunnel-table context
Context	network-instance name <i>string</i> tunnel-table
Tree	tunnel-table
Configurable	False
Platforms	Supported on all platforms

ipv4

Description	The container for the IPv4 tunnels associated with the network instance.
Context	network-instance name <i>string</i> tunnel-table ipv4

Tree	ipv4
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> tunnel-table ipv4 statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-tunnels *number*

Description	The total number of tunnels, belonging to this address family, that are active.
Context	network-instance name <i>string</i> tunnel-table ipv4 statistics active-tunnels <i>number</i>
Tree	active-tunnels
Configurable	False
Platforms	Supported on all platforms

inactive-tunnels *number*

Description	The total number of tunnels, belonging to this address family, that are inactive (not programmed).
Context	network-instance name <i>string</i> tunnel-table ipv4 statistics inactive-tunnels <i>number</i>
Tree	inactive-tunnels
Configurable	False
Platforms	Supported on all platforms

total-tunnels *number*

Description	The total number of tunnels, active and inactive, belonging to this address family
Context	network-instance name <i>string</i> tunnel-table ipv4 statistics total-tunnels <i>number</i>
Tree	total-tunnels

Default	0
Configurable	False
Platforms	Supported on all platforms

tunnel *ipv4-prefix string type identityref owner string id number*

Description	Enter the tunnel list instance
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number
Tree	tunnel
Configurable	False
Platforms	Supported on all platforms

ipv4-prefix *string*

Description	The IPv4 prefix associated with the endpoint of the tunnel.
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number
Configurable	False
Platforms	Supported on all platforms

type *identityref*

Description	The tunnel (encapsulation) type
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number
Options	<ul style="list-style-type: none"> • sr-isis Segment routing using MPLS dataplane, programmed by IS-IS • sr-ospfv2 Segment routing using MPLS dataplane, programmed by OSPFv2 • sr-ospfv3 Segment routing using MPLS dataplane, programmed by OSPFv3 • vxlan Tunnels based on VXLAN encapsulation
Configurable	False
Platforms	Supported on all platforms

owner string

Description	The name of the application that submitted the tunnel to TTM
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number
Configurable	False
Platforms	Supported on all platforms

id number

Description	An owner-assigned index value that is unique for each of the tunnels terminating at a particular prefix.
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number
Configurable	False
Platforms	Supported on all platforms

encapsulation-type keyword

Description	The type of encapsulation used by the tunnel.
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number encapsulation-type keyword
Tree	encapsulation-type
Options	<ul style="list-style-type: none"> • vxlan • mpls
Configurable	False
Platforms	Supported on all platforms

fib-programming

Description	Container for state related to the FIB programming of the tunnel
Context	network-instance name string tunnel-table ipv4 tunnel ipv4-prefix string type identityref owner string id number fib-programming
Tree	fib-programming
Configurable	False
Platforms	Supported on all platforms

not-programmed-reason *keyword*

Description	The reason why the tunnel is not programmed
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number fib-programming not-programmed-reason <i>keyword</i>
Tree	not-programmed-reason
Options	<ul style="list-style-type: none"> • out-of-tunnel-resources
Configurable	False
Platforms	Supported on all platforms

status *keyword*

Description	The status of the tunnel programming
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number fib-programming status <i>keyword</i>
Tree	status
Options	<ul style="list-style-type: none"> • active The tunnel is active and programmed into the datapath. • inactive The tunnel is inactive and not programmed into the datapath.
Configurable	False
Platforms	Supported on all platforms

last-app-update *string*

Description	The date and time of the last update of this tunnel by the owning application or protocol.
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number last-app-update <i>string</i>
Tree	last-app-update
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

metric *number*

Description	The metric of the tunnel.
--------------------	---------------------------

Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number metric <i>number</i>
Tree	metric
Configurable	False
Platforms	Supported on all platforms

next-hop-group *reference*

Description	Leaf reference to a next-hop-group that has the direct next-hops towards the tunnel far-end
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number next-hop-group reference
Tree	next-hop-group
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

preference *number*

Description	The tunnel table preference.
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number preference <i>number</i>
Tree	preference
Configurable	False
Platforms	Supported on all platforms

vxlan

Description	Enter the vxlan context
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan
Tree	vxlan
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan destination-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	destination-address
Configurable	False
Platforms	Supported on all platforms

destination-udp-port *number*

Description	The destination UDP port number written into the outer IP/UDP header of VXLAN packets associated with this tunnel and originated by this router.
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan destination-udp-port <i>number</i>
Tree	destination-udp-port
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP address that identifies the local VXLAN Termination Endpoint (VTEP).
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan source-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	source-address
Configurable	False
Platforms	Supported on all platforms

time-to-live *number*

Description	The Time To Live (TTL) value written into the outer IP header of VXLAN packets associated with this tunnel and originated by this router.
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel ipv4-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan time-to-live <i>number</i>
Tree	time-to-live
Configurable	False
Platforms	Supported on all platforms

tunnel-summary

Description	Tunnel summary information
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel-summary
Tree	tunnel-summary
Configurable	False
Platforms	Supported on all platforms

tunnel-type *type identityref*

Description	Enter the tunnel-type list instance
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel-summary tunnel-type <i>type identityref</i>
Tree	tunnel-type
Configurable	False
Platforms	Supported on all platforms

type *identityref*

Description	Tunneling encapsulation format
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel-summary tunnel-type <i>type identityref</i>
Options	<ul style="list-style-type: none"> • <code>sr-isis</code> Segment routing using MPLS dataplane, programmed by IS-IS • <code>sr-ospfv2</code> Segment routing using MPLS dataplane, programmed by OSPFv2 • <code>sr-ospfv3</code> Segment routing using MPLS dataplane, programmed by OSPFv3 • <code>vxlan</code> Tunnels based on VXLAN encapsulation
Configurable	False
Platforms	Supported on all platforms

active-tunnels *number*

Description	The total number of tunnels, using this encapsulation type, that are active.
--------------------	--

Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel-summary tunnel-type type identityref active-tunnels <i>number</i>
Tree	active-tunnels
Configurable	False
Platforms	Supported on all platforms

inactive-tunnels *number*

Description	The total number of tunnels, using this encapsulation type, that are inactive (not programmed).
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel-summary tunnel-type type identityref inactive-tunnels <i>number</i>
Tree	inactive-tunnels
Configurable	False
Platforms	Supported on all platforms

total-tunnels *number*

Description	The total number of tunnels, active and inactive, using this encapsulation type.
Context	network-instance name <i>string</i> tunnel-table ipv4 tunnel-summary tunnel-type type identityref total-tunnels <i>number</i>
Tree	total-tunnels
Default	0
Configurable	False
Platforms	Supported on all platforms

ipv6

Description	The container for the IPv6 tunnels associated with the network instance.
Context	network-instance name <i>string</i> tunnel-table ipv6
Tree	ipv6
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
--------------------	------------------------------

Context	network-instance name <i>string</i> tunnel-table ipv6 statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-tunnels *number*

Description	The total number of tunnels, belonging to this address family, that are active.
Context	network-instance name <i>string</i> tunnel-table ipv6 statistics active-tunnels <i>number</i>
Tree	active-tunnels
Configurable	False
Platforms	Supported on all platforms

inactive-tunnels *number*

Description	The total number of tunnels, belonging to this address family, that are inactive (not programmed).
Context	network-instance name <i>string</i> tunnel-table ipv6 statistics inactive-tunnels <i>number</i>
Tree	inactive-tunnels
Configurable	False
Platforms	Supported on all platforms

total-tunnels *number*

Description	The total number of tunnels, active and inactive, belonging to this address family
Context	network-instance name <i>string</i> tunnel-table ipv6 statistics total-tunnels <i>number</i>
Tree	total-tunnels
Default	0
Configurable	False
Platforms	Supported on all platforms

tunnel [ipv6-prefix](#) *string* [type](#) [identityref](#) [owner](#) *string* [id](#) *number*

Description	Enter the tunnel list instance
--------------------	--------------------------------

Context	network-instance name string tunnel-table ipv6 tunnel ipv6-prefix string type identityref owner string id number
Tree	tunnel
Configurable	False
Platforms	Supported on all platforms

ipv6-prefix string

Description	The IPv6 prefix associated with the endpoint of the tunnel.
Context	network-instance name string tunnel-table ipv6 tunnel ipv6-prefix string type identityref owner string id number
Configurable	False
Platforms	Supported on all platforms

type identityref

Description	The tunnel (encapsulation) type
Context	network-instance name string tunnel-table ipv6 tunnel ipv6-prefix string type identityref owner string id number
Options	<ul style="list-style-type: none"> • sr-isis Segment routing using MPLS dataplane, programmed by IS-IS • sr-ospfv2 Segment routing using MPLS dataplane, programmed by OSPFv2 • sr-ospfv3 Segment routing using MPLS dataplane, programmed by OSPFv3 • vxlan Tunnels based on VXLAN encapsulation
Configurable	False
Platforms	Supported on all platforms

owner string

Description	The name of the application that submitted the tunnel to TTM
Context	network-instance name string tunnel-table ipv6 tunnel ipv6-prefix string type identityref owner string id number
Configurable	False
Platforms	Supported on all platforms

id number

Description	An owner-assigned index value that is unique for each of the tunnels terminating at a particular prefix.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string type identityref owner string id number</i>
Configurable	False
Platforms	Supported on all platforms

encapsulation-type keyword

Description	The type of encapsulation used by the tunnel.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string type identityref owner string id number encapsulation-type keyword</i>
Tree	encapsulation-type
Options	<ul style="list-style-type: none"> • vxlan • mpls
Configurable	False
Platforms	Supported on all platforms

fib-programming

Description	Container for state related to the FIB programming of the tunnel
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string type identityref owner string id number fib-programming</i>
Tree	fib-programming
Configurable	False
Platforms	Supported on all platforms

not-programmed-reason keyword

Description	The reason why the tunnel is not programmed
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string type identityref owner string id number fib-programming not-programmed-reason keyword</i>
Tree	not-programmed-reason
Options	<ul style="list-style-type: none"> • out-of-tunnel-resources
Configurable	False

Platforms Supported on all platforms

status *keyword*

Description The status of the tunnel programming

Context [network-instance name](#) *string* [tunnel-table ipv6 tunnel ipv6-prefix](#) *string type identityref owner string id number fib-programming status keyword*

Tree [status](#)

Options

- active
The tunnel is active and programmed into the datapath.
- inactive
The tunnel is inactive and not programmed into the datapath.

Configurable False

Platforms Supported on all platforms

last-app-update *string*

Description The date and time of the last update of this tunnel by the owning application or protocol.

Context [network-instance name](#) *string* [tunnel-table ipv6 tunnel ipv6-prefix](#) *string type identityref owner string id number last-app-update string*

Tree [last-app-update](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

metric *number*

Description The metric of the tunnel.

Context [network-instance name](#) *string* [tunnel-table ipv6 tunnel ipv6-prefix](#) *string type identityref owner string id number metric number*

Tree [metric](#)

Configurable False

Platforms Supported on all platforms

next-hop-group *reference*

Description	Leaf reference to a next-hop-group that has the direct next-hops towards the tunnel far-end
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number next-hop-group reference
Tree	next-hop-group
Reference	network-instance name <i>string</i> route-table next-hop-group index <i>number</i>
Configurable	False
Platforms	Supported on all platforms

preference *number*

Description	The tunnel table preference.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number preference number
Tree	preference
Configurable	False
Platforms	Supported on all platforms

vxlan

Description	Enter the vxlan context
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan
Tree	vxlan
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan destination-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	destination-address
Configurable	False
Platforms	Supported on all platforms

destination-udp-port *number*

Description	The destination UDP port number written into the outer IP/UDP header of VXLAN packets associated with this tunnel and originated by this router.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan destination-udp-port <i>number</i>
Tree	destination-udp-port
Configurable	False
Platforms	Supported on all platforms

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

Description	The IP address that identifies the local VXLAN Termination Endpoint (VTEP).
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan source-address (<i>ipv4-address ipv6-address</i>)
Tree	source-address
Configurable	False
Platforms	Supported on all platforms

time-to-live *number*

Description	The Time To Live (TTL) value written into the outer IP header of VXLAN packets associated with this tunnel and originated by this router.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel ipv6-prefix <i>string</i> type identityref owner <i>string</i> id number vxlan time-to-live <i>number</i>
Tree	time-to-live
Configurable	False
Platforms	Supported on all platforms

tunnel-summary

Description	Tunnel summary information
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel-summary
Tree	tunnel-summary
Configurable	False
Platforms	Supported on all platforms

tunnel-type *type identityref*

Description	Enter the tunnel-type list instance
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel-summary tunnel-type <i>type identityref</i>
Tree	tunnel-type
Configurable	False
Platforms	Supported on all platforms

type *identityref*

Description	Tunneling encapsulation format
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel-summary tunnel-type <i>type identityref</i>
Options	<ul style="list-style-type: none"> • sr-isis Segment routing using MPLS dataplane, programmed by IS-IS • sr-ospfv2 Segment routing using MPLS dataplane, programmed by OSPFv2 • sr-ospfv3 Segment routing using MPLS dataplane, programmed by OSPFv3 • vxlan Tunnels based on VXLAN encapsulation
Configurable	False
Platforms	Supported on all platforms

active-tunnels *number*

Description	The total number of tunnels, using this encapsulation type, that are active.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel-summary tunnel-type <i>type identityref</i> active-tunnels <i>number</i>
Tree	active-tunnels
Configurable	False
Platforms	Supported on all platforms

inactive-tunnels *number*

Description	The total number of tunnels, using this encapsulation type, that are inactive (not programmed).
--------------------	---

Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel-summary tunnel-type type identityref inactive-tunnels <i>number</i>
Tree	inactive-tunnels
Configurable	False
Platforms	Supported on all platforms

total-tunnels *number*

Description	The total number of tunnels, active and inactive, using this encapsulation type.
Context	network-instance name <i>string</i> tunnel-table ipv6 tunnel-summary tunnel-type type identityref total-tunnels <i>number</i>
Tree	total-tunnels
Default	0
Configurable	False
Platforms	Supported on all platforms

type *identityref*

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
Context	network-instance name <i>string</i> type <i>identityref</i>
Tree	type
Default	default
Options	<ul style="list-style-type: none"> • host A special routing instances that refers to the hosts network instance (i.e. the network namespace of PID 1) • default A special routing instance which acts as the 'default' 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
Platforms	Supported on all platforms

udp

Description	State for UDP datagrams routed using the route tables of this network instance.
Context	network-instance name <i>string</i> udp
Tree	udp
Configurable	False
Platforms	Supported on all platforms

listening-application [local-address](#) (*ipv4-address* | *ipv6-address*) [local-port](#) *number*

Description	List of applications that are listening on a particular UDP port bound to the network-instance.
Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i>
Tree	listening-application
Configurable	False
Platforms	Supported on all platforms

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

Description	The local IP address accepted by the application. An all-zeroes value for the <i>ipv4-address</i> means that any IPv4 address is accepted. An all-zeroes value for the <i>ipv6-address</i> means that any IPv6 address is accepted.
Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i>
Configurable	False
Platforms	Supported on all platforms

local-port *number*

Description	The local port number accepted by the application.
Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i>
Range	0 to 65535
Configurable	False
Platforms	Supported on all platforms

process-id *number*

Description	The process ID of the application that owns the socket.
Context	network-instance name <i>string</i> udp listening-application local-address (<i>ipv4-address</i> <i>ipv6-address</i>) local-port <i>number</i> process-id <i>number</i>
Tree	process-id
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> udp statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

ignored-multicast-packets *number*

Description	The total number of ignored multicast UDP datagrams.
Context	network-instance name <i>string</i> udp statistics ignored-multicast-packets <i>number</i>
Tree	ignored-multicast-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-checksum-errors *number*

Description	Increased when a received UDP packet has an invalid checksum.
Context	network-instance name <i>string</i> udp statistics in-checksum-errors <i>number</i>
Tree	in-checksum-errors
Default	0
Configurable	False
Platforms	Supported on all platforms

in-error-packets *number*

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.
Context	network-instance name <i>string</i> udp statistics in-error-packets <i>number</i>
Tree	in-error-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-no-open-ports-packets *number*

Description	The total number of received UDP datagrams for which there was no application at the destination port.
Context	network-instance name <i>string</i> udp statistics in-no-open-ports-packets <i>number</i>
Tree	in-no-open-ports-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

in-packets *number*

Description	The total number of UDP datagrams delivered to UDP users.
Context	network-instance name <i>string</i> udp statistics in-packets <i>number</i>
Tree	in-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

out-packets *number*

Description	The total number of UDP datagrams sent from this network instance.
Context	network-instance name <i>string</i> udp statistics out-packets <i>number</i>
Tree	out-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

receive-buffer-errors *number*

Description	Increased when memory cannot be allocated to process an incoming UDP packet.
Context	network-instance name <i>string</i> udp statistics receive-buffer-errors <i>number</i>
Tree	receive-buffer-errors
Default	0
Configurable	False
Platforms	Supported on all platforms

send-buffer-errors *number*

Description	Increased when memory cannot be allocated to send a UDP packet.
Context	network-instance name <i>string</i> udp statistics send-buffer-errors <i>number</i>
Tree	send-buffer-errors
Default	0
Configurable	False
Platforms	Supported on all platforms

vxlan-interface [name](#) *string*

Description	List of vxlan-interfaces used by this network-instance
Context	network-instance name <i>string</i> vxlan-interface name <i>string</i>
Tree	vxlan-interface
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	1

name *string*

Description	Identifier of vxlan-interface used in this network-instance
Context	network-instance name <i>string</i> vxlan-interface name <i>string</i>
String Length	8 to 17
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-down-reason *keyword*

Description	The reason for the vxlan-interface being down in the network-instance
Context	network-instance name <i>string</i> vxlan-interface name <i>string</i> oper-down-reason <i>keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • vxlan-tunnel-down • net-inst-down • vxlan-if-default-net-inst-source-address-missing • vxlan-if-default-net-inst-source-if-down • vrf-type-mismatch
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-state *keyword*

Description	The operational state of this vxlan-interface.
Context	network-instance name <i>string</i> vxlan-interface name <i>string</i> oper-state <i>keyword</i>
Tree	oper-state
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

- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

7 platform

```

platform
+ chassis
- clei-code string
- failure-reason string
- hw-mac-address string
- last-boot-type string
- last-booted string
- last-change 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
- cgroup name string
- cpuacct-statistics
- system number
- user number
- memory-statistics
- anon number
- anon-thp number
- current number
- current-swap number
- file number
- file-dirty number
- file-writeback number
- kernel-stack number
- memory-events
- high number
- low number
- max number
- oom number
- oom-kill number
- slab number

```

```

- sock number
- 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 number
  - 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-reason keyword
  - 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
- free number
- reserved number
- sram
  - free number
  - used number
- used number
- datapath
  - asic
    - resource name identityref
    - free-entries number
    - used-entries number
    - used-percent number
  - xdp
    - resource name identityref
    - free-entries number
    - used-entries number
    - used-percent number
+ fabric
- availability number
- utilization-egress number
- utilization-ingress number
- mtu
  - resource name identityref
  - free number
  - used number
+ pipeline index (number | keyword)
- datapath
  - xdp
    - resource name identityref
    - free-entries number
    - used-entries number
    - used-percent number
- pipeline-counters
  - host-interface-block
    - packet-extraction
      - extracted-octets number
      - extracted-packets number
      - extraction-reason reason identityref
        - extracted-octets number
        - extracted-packets number
      - forwarding-class fc keyword
        - extracted-octets number
        - extracted-packets number
- qos
  - resource name identityref
  - free number
  - used number
- tcam
  - resource name identityref
  - free-dynamic number
  - free-static 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-reason keyword
  - 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-management
+ tcam
+ unified-forwarding-resources
  - allocated-extra-ip-host-entries number
  - allocated-extra-mac-entries number
  + alpm keyword
  + ipv6-128bit-lpm-entries number
  + requested-extra-ip-host-entries number
  - xdp-restart-required boolean
+ resource-monitoring
+ acl
  + resource name identityref
  + falling-threshold-log number
  + rising-threshold-log number
+ datapath
+ asic
  + resource name identityref
  + falling-threshold-log number
  + rising-threshold-log number
+ xdp

```

```
+ 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
```

7.1 platform Descriptions

platform

Description	Enclosing container for platform components
Context	platform
Tree	platform
Configurable	True
Platforms	Supported on all platforms

chassis

Description	Top-level container for chassis configuration and state
Context	platform chassis
Tree	chassis
Configurable	True
Platforms	Supported on all platforms

clei-code *string*

Description	The Common Language Identification Code for this component
Context	platform chassis clei-code string
Tree	clei-code
Configurable	False
Platforms	Supported on all platforms

failure-reason *string*

Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Context	platform chassis failure-reason string
Tree	failure-reason
Configurable	False
Platforms	Supported on all platforms

hw-mac-address *string*

Description	The chassis MAC address Read from hardware, or derived from the systems UUID
Context	platform chassis hw-mac-address <i>string</i>
Tree	hw-mac-address
Configurable	False
Platforms	Supported on all platforms

last-boot-type *string*

Description	The type of boot the chassis initialized from This field indicates what type of reboot occurred, whether it be warm, normal, or otherwise.
Context	platform chassis last-boot-type <i>string</i>
Tree	last-boot-type
Configurable	False
Platforms	Supported on all platforms

last-booted *string*

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
Context	platform chassis last-booted <i>string</i>
Tree	last-booted
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-change *string*

Description	The date and time this component last changed state
Context	platform chassis last-change <i>string</i>
Tree	last-change
String Length	20 to 32
Configurable	False

Platforms Supported on all platforms

manufactured-date *string*

Description The date this component was manufactured
Context [platform chassis manufactured-date](#) *string*
Tree [manufactured-date](#)
Configurable False
Platforms Supported on all platforms

oper-state *keyword*

Description The operational state of this component
Context [platform chassis oper-state](#) *keyword*
Tree [oper-state](#)
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state

- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
 - waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
- Configurable** False
- Platforms** Supported on all platforms

part-number *string*

- Description** Part number for this component
- Context** [platform chassis part-number](#) *string*
- Tree** [part-number](#)
- Configurable** False
- Platforms** Supported on all platforms

power

- Description** Top-level container for chassis-wide power state
- Context** [platform chassis power](#)
- Tree** [power](#)
- Configurable** True
- Platforms** Supported on all platforms

control

- Description** Top-level container for power usage of control modules
- Context** [platform chassis power control](#)
- Tree** [control](#)
- Configurable** False
- Platforms** 7250 IXR-10, 7250 IXR-6

allocated number

Description	Allocated power
Context	platform chassis power control allocated number
Tree	allocated
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peak number

Description	Peak power used
Context	platform chassis power control peak number
Tree	peak
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	Used power
Context	platform chassis power control used number
Tree	used
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fabric

Description	Top-level container for power usage of fabric modules
Context	platform chassis power fabric
Tree	fabric
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

allocated number

Description	Allocated power
Context	platform chassis power fabric allocated number
Tree	allocated

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peak number

Description	Peak power used
Context	platform chassis power fabric peak number
Tree	peak
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	Used power
Context	platform chassis power fabric used number
Tree	used
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fan-tray

Description	Top-level container for power usage of fan-trays
Context	platform chassis power fan-tray
Tree	fan-tray
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

allocated number

Description	Allocated power
Context	platform chassis power fan-tray allocated number
Tree	allocated
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peak number

Description	Peak power used
Context	platform chassis power fan-tray peak number
Tree	peak
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	Used power
Context	platform chassis power fan-tray used number
Tree	used
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

linecard

Description	Top-level container for power usage of linecard modules
Context	platform chassis power linecard
Tree	linecard
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

allocated number

Description	Allocated power
Context	platform chassis power linecard allocated number
Tree	allocated
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

peak number

Description	Peak power used
Context	platform chassis power linecard peak number
Tree	peak

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	Used power
Context	platform chassis power linecard used number
Tree	used
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

total

Description	Top-level container for total power usage and capacity
Context	platform chassis power total
Tree	total
Configurable	False
Platforms	Supported on all platforms

allocated number

Description	Allocated power
Context	platform chassis power total allocated number
Tree	allocated
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

capacity number

Description	Total power capacity provided by all power supplies
Context	platform chassis power total capacity number
Tree	capacity
Configurable	False
Platforms	Supported on all platforms

peak number

Description	Peak power used
Context	platform chassis power total peak number
Tree	peak
Configurable	False
Platforms	Supported on all platforms

used number

Description	Used power
Context	platform chassis power total used number
Tree	used
Configurable	False
Platforms	Supported on all platforms

removable boolean

Description	Details if this component can be removed from the system
Context	platform chassis removable boolean
Tree	removable
Configurable	False
Platforms	Supported on all platforms

serial-number string

Description	The serial number for this component
Context	platform chassis serial-number string
Tree	serial-number
Configurable	False
Platforms	Supported on all platforms

slots number

Description	The number of line card slots supported by the chassis
Context	platform chassis slots number
Tree	slots

Configurable	False
Platforms	Supported on all platforms

type *string*

Description	The chassis type
Context	platform chassis type <i>string</i>
Tree	type
Configurable	False
Platforms	Supported on all platforms

control [slot](#) *string*

Description	Top-level container for control module configuration and state
Context	platform control slot <i>string</i>
Tree	control
Configurable	True
Platforms	Supported on all platforms

slot *string*

Description	Slot identifier for the control module This is set to 'A' for systems without removable control modules.
Context	platform control slot <i>string</i>
Configurable	True
Platforms	Supported on all platforms

cgroup [name](#) *string*

Description	List of cgroups present in the system
Context	platform control slot <i>string</i> cgroup name <i>string</i>
Tree	cgroup
Configurable	False
Platforms	Supported on all platforms

name *string*

Description	Name of the cgroup, as defined by its directory location in the filesystem
Context	platform control slot <i>string</i> cgroup name <i>string</i>
Configurable	False
Platforms	Supported on all platforms

cpuacct-statistics

Description	Top-level container for cgroup cpuacct statistics
Context	platform control slot <i>string</i> cgroup name <i>string</i> cpuacct-statistics
Tree	cpuacct-statistics
Configurable	False
Platforms	Supported on all platforms

system *number*

Description	CPU usage user system
Context	platform control slot <i>string</i> cgroup name <i>string</i> cpuacct-statistics system <i>number</i>
Tree	system
Units	useconds
Configurable	False
Platforms	Supported on all platforms

user *number*

Description	CPU usage user mode
Context	platform control slot <i>string</i> cgroup name <i>string</i> cpuacct-statistics user <i>number</i>
Tree	user
Units	useconds
Configurable	False
Platforms	Supported on all platforms

memory-statistics

Description	Top-level container for cgroup memory statistics
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics

Tree	memory-statistics
Configurable	False
Platforms	Supported on all platforms

anon number

Description	Amount of memory used in anonymous mappings such as brk(), sbrk(), and mmap(MAP_ANONYMOUS)
Context	platform control slot string cgroup name string memory-statistics anon number
Tree	anon
Units	bytes
Configurable	False
Platforms	Supported on all platforms

anon-thp number

Description	Amount of memory used in anonymous mappings backed by transparent hugepages
Context	platform control slot string cgroup name string memory-statistics anon-thp number
Tree	anon-thp
Units	bytes
Configurable	False
Platforms	Supported on all platforms

current number

Description	The total amount of memory currently being used by the cgroup and its descendants. Read from memory.current
Context	platform control slot string cgroup name string memory-statistics current number
Tree	current
Units	bytes
Configurable	False
Platforms	Supported on all platforms

current-swap *number*

Description	The total amount of swap currently being used by the cgroup and its descendants. Read from <code>memory.swap.current</code>
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics current-swap <i>number</i>
Tree	current-swap
Units	bytes
Configurable	False
Platforms	Supported on all platforms

file *number*

Description	Amount of memory used to cache filesystem data, including tmpfs and shared memory
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics file <i>number</i>
Tree	file
Units	bytes
Configurable	False
Platforms	Supported on all platforms

file-dirty *number*

Description	Amount of cached filesystem data that was modified but not yet written back to disk
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics file-dirty <i>number</i>
Tree	file-dirty
Units	bytes
Configurable	False
Platforms	Supported on all platforms

file-writeback *number*

Description	Amount of cached filesystem data that was modified and is currently being written back to disk
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics file-writeback <i>number</i>
Tree	file-writeback

Units	bytes
Configurable	False
Platforms	Supported on all platforms

kernel-stack *number*

Description	Amount of memory allocated to kernel stacks
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics kernel-stack number
Tree	kernel-stack
Units	bytes
Configurable	False
Platforms	Supported on all platforms

memory-events

Description	Top-level container for cgroup memory events
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics memory-events
Tree	memory-events
Configurable	False
Platforms	Supported on all platforms

high *number*

Description	The number of times processes of the cgroup are throttled and routed to perform direct memory reclaim because the high memory boundary was exceeded.
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics memory-events high number
Tree	high
Configurable	False
Platforms	Supported on all platforms

low *number*

Description	The number of times the cgroup is reclaimed due to high memory pressure even though its usage is under the low boundary.
--------------------	--

Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics memory-events low <i>number</i>
Tree	low
Configurable	False
Platforms	Supported on all platforms

max *number*

Description	The number of times the cgroup's memory usage was about to go over the max boundary
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics memory-events max <i>number</i>
Tree	max
Configurable	False
Platforms	Supported on all platforms

oom *number*

Description	The number of time the cgroup's memory usage had reached the limit and allocation was about to fail
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics memory-events oom <i>number</i>
Tree	oom
Configurable	False
Platforms	Supported on all platforms

oom-kill *number*

Description	The number of processes belonging to this cgroup killed by any kind of out-of-memory killer
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics memory-events oom-kill <i>number</i>
Tree	oom-kill
Configurable	False
Platforms	Supported on all platforms

slab *number*

Description	Amount of memory used for storing in-kernel data structures
--------------------	---

Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics slab number
Tree	slab
Units	bytes
Configurable	False
Platforms	Supported on all platforms

sock number

Description	Amount of memory used in network transmission buffers
Context	platform control slot <i>string</i> cgroup name <i>string</i> memory-statistics sock number
Tree	sock
Units	bytes
Configurable	False
Platforms	Supported on all platforms

clei-code string

Description	The Common Language Identification Code for this component
Context	platform control slot <i>string</i> clei-code <i>string</i>
Tree	clei-code
Configurable	False
Platforms	Supported on all platforms

cpu index (keyword | number)

Description	List of all CPUs in the system
Context	platform control slot <i>string</i> cpu index (keyword number)
Tree	cpu
Configurable	False
Platforms	Supported on all platforms

index (keyword | number)

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.

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>)
Options	<ul style="list-style-type: none"> all Index value indicating all CPUs in the system
Configurable	False
Platforms	Supported on all platforms

architecture *keyword*

Description	Architecture supported by the CPU
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) architecture <i>keyword</i>
Tree	architecture
Options	<ul style="list-style-type: none"> x86_64
Configurable	False
Platforms	Supported on all platforms

hardware-interrupt

Description	Time spent servicing hardware interrupts
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt
Tree	hardware-interrupt
Configurable	False
Platforms	Supported on all platforms

average-1 *number*

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt average-1 <i>number</i>
Tree	average-1
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 *number*

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt average-15 <i>number</i>
Tree	average-15
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 *number*

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt average-5 <i>number</i>
Tree	average-5
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

instant *number*

Description	The instantaneous percentage value
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) hardware-interrupt instant <i>number</i>
Tree	instant
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

idle

Description	Time spent idle
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) idle
Tree	idle
Configurable	False
Platforms	Supported on all platforms

average-1 *number*

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) idle average-1 <i>number</i>
Tree	average-1
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 *number*

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) idle average-15 <i>number</i>
Tree	average-15
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 *number*

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) idle average-5 <i>number</i>
Tree	average-5
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

instant *number*

Description	The instantaneous percentage value
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) idle instant <i>number</i>
Tree	instant
Range	0 to 100
Configurable	False

Platforms Supported on all platforms

iowait

Description Time spent idle, waiting for an outstanding disk I/O request

Context [platform control slot string cpu index \(keyword | number\) iowait](#)

Tree [iowait](#)

Configurable False

Platforms Supported on all platforms

average-1 number

Description The arithmetic mean value of this statistic over the last minute

Context [platform control slot string cpu index \(keyword | number\) iowait average-1 number](#)

Tree [average-1](#)

Range 0 to 100

Configurable False

Platforms Supported on all platforms

average-15 number

Description The arithmetic mean value of this statistic over the last fifteen minutes

Context [platform control slot string cpu index \(keyword | number\) iowait average-15 number](#)

Tree [average-15](#)

Range 0 to 100

Configurable False

Platforms Supported on all platforms

average-5 number

Description The arithmetic mean value of this statistic over the last five minutes

Context [platform control slot string cpu index \(keyword | number\) iowait average-5 number](#)

Tree [average-5](#)

Range 0 to 100

Configurable	False
Platforms	Supported on all platforms

instant number

Description	The instantaneous percentage value
Context	platform control slot string cpu index (keyword number) iowait instant number
Tree	instant
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

nice

Description	Time spent running low-priority (niced) user processes
Context	platform control slot string cpu index (keyword number) nice
Tree	nice
Configurable	False
Platforms	Supported on all platforms

average-1 number

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot string cpu index (keyword number) nice average-1 number
Tree	average-1
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 number

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot string cpu index (keyword number) nice average-15 number
Tree	average-15

Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 *number*

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) nice average-5 <i>number</i>
Tree	average-5
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

instant *number*

Description	The instantaneous percentage value
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) nice instant <i>number</i>
Tree	instant
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

software-interrupt

Description	Time spent servicing software interrupts
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) software-interrupt
Tree	software-interrupt
Configurable	False
Platforms	Supported on all platforms

average-1 *number*

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot <i>string</i> cpu index (<i>keyword</i> <i>number</i>) software-interrupt average-1 <i>number</i>
Tree	average-1

Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 *number*

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt average-15 <i>number</i>
Tree	average-15
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 *number*

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt average-5 <i>number</i>
Tree	average-5
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

instant *number*

Description	The instantaneous percentage value
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) software-interrupt instant <i>number</i>
Tree	instant
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

speed *decimal-number*

Description	Capable speed of the CPU
--------------------	--------------------------

Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) speed <i>decimal-number</i>
Tree	speed
Units	gigahertz
Configurable	False
Platforms	Supported on all platforms

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.
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system
Tree	system
Configurable	False
Platforms	Supported on all platforms

average-1 *number*

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system average-1 <i>number</i>
Tree	average-1
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 *number*

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) system average-15 <i>number</i>
Tree	average-15
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 number

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot string cpu index (keyword number) system average-5 number
Tree	average-5
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

instant number

Description	The instantaneous percentage value
Context	platform control slot string cpu index (keyword number) system instant number
Tree	instant
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

total

Description	Total CPU utilization
Context	platform control slot string cpu index (keyword number) total
Tree	total
Configurable	False
Platforms	Supported on all platforms

average-1 number

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot string cpu index (keyword number) total average-1 number
Tree	average-1
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 *number*

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total average-15 number
Tree	average-15
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 *number*

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total average-5 number
Tree	average-5
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

instant *number*

Description	The instantaneous percentage value
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) total instant number
Tree	instant
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

type *string*

Description	Model name of the CPU
Context	platform control slot <i>string</i> cpu index (<i>keyword number</i>) type string
Tree	type
Configurable	False
Platforms	Supported on all platforms

user

Description	Time spent executing at the user level This can otherwise be known as application or user space time.
Context	platform control slot string cpu index (keyword number) user
Tree	user
Configurable	False
Platforms	Supported on all platforms

average-1 number

Description	The arithmetic mean value of this statistic over the last minute
Context	platform control slot string cpu index (keyword number) user average-1 number
Tree	average-1
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-15 number

Description	The arithmetic mean value of this statistic over the last fifteen minutes
Context	platform control slot string cpu index (keyword number) user average-15 number
Tree	average-15
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

average-5 number

Description	The arithmetic mean value of this statistic over the last five minutes
Context	platform control slot string cpu index (keyword number) user average-5 number
Tree	average-5
Range	0 to 100
Configurable	False

Platforms Supported on all platforms

instant *number*

Description The instantaneous percentage value

Context [platform control slot](#) *string* [cpu index](#) (*keyword | number*) [user instant](#) *number*

Tree [instant](#)

Range 0 to 100

Configurable False

Platforms Supported on all platforms

disk name *string*

Description List of disks present in the system

Context [platform control slot](#) *string* [disk name](#) *string*

Tree [disk](#)

Configurable False

Platforms Supported on all platforms

name *string*

Description Name of the disk, as defined by its physical location in the system

Context [platform control slot](#) *string* [disk name](#) *string*

Configurable False

Platforms Supported on all platforms

model-number *string*

Description Model name of the disk

Context [platform control slot](#) *string* [disk name](#) *string* [model-number](#) *string*

Tree [model-number](#)

Configurable False

Platforms Supported on all platforms

partition name *string*

Description List of partitions available on this disk

Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i>
Tree	partition
Configurable	False
Platforms	Supported on all platforms

name *string*

Description	Name of the partition
Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i>
Configurable	False
Platforms	Supported on all platforms

free *number*

Description	Space free on the partition
Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> free <i>number</i>
Tree	free
Units	bytes
Configurable	False
Platforms	Supported on all platforms

mount-point *string*

Description	Path to where this partition is mounted
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
Configurable	False
Platforms	Supported on all platforms

mount-status *keyword*

Description	Current mount status of this partition
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
Options	<ul style="list-style-type: none"> ro

- Partition is currently mounted read-only
- rw
- Partition is currently mounted read-write

Configurable	False
Platforms	Supported on all platforms

percent-used *number*

Description	Percentage of the partition in use
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
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

size *number*

Description	Size of the partition
Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> size <i>number</i>
Tree	size
Units	bytes
Configurable	False
Platforms	Supported on all platforms

used *number*

Description	Space used on the partition
Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> used <i>number</i>
Tree	used
Units	bytes
Configurable	False
Platforms	Supported on all platforms

uuid *string*

Description	UUID of the partition
Context	platform control slot <i>string</i> disk name <i>string</i> partition name <i>string</i> uuid <i>string</i>
Tree	uuid
Configurable	False
Platforms	Supported on all platforms

serial-number *string*

Description	Serial number of the disk
Context	platform control slot <i>string</i> disk name <i>string</i> serial-number <i>string</i>
Tree	serial-number
Configurable	False
Platforms	Supported on all platforms

size *number*

Description	Total size of the disk
Context	platform control slot <i>string</i> disk name <i>string</i> size <i>number</i>
Tree	size
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Top-level container for disk statistics
Context	platform control slot <i>string</i> disk name <i>string</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

read-per-second *decimal-number*

Description	Indicates the amount of data read from the device per second
Context	platform control slot <i>string</i> disk name <i>string</i> statistics read-per-second <i>decimal-number</i>
Tree	read-per-second

Units	bytes
Configurable	False
Platforms	Supported on all platforms

transfers-per-second *decimal-number*

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.
Context	platform control slot <i>string</i> disk name <i>string</i> statistics transfers-per-second <i>decimal-number</i>
Tree	transfers-per-second
Configurable	False
Platforms	Supported on all platforms

utilization *number*

Description	The current tps utilization of the disk, expressed as a percentage
Context	platform control slot <i>string</i> disk name <i>string</i> statistics utilization <i>number</i>
Tree	utilization
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

written-per-second *decimal-number*

Description	Indicates the amount of data written to the device per second
Context	platform control slot <i>string</i> disk name <i>string</i> statistics written-per-second <i>decimal-number</i>
Tree	written-per-second
Units	bytes
Configurable	False
Platforms	Supported on all platforms

type *keyword*

Description	Type of disk
--------------------	--------------

Context	platform control slot <i>string</i> disk name <i>string</i> type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • compactflash • ssd • hdd • usb
Configurable	False
Platforms	Supported on all platforms

failure-reason *string*

Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Context	platform control slot <i>string</i> failure-reason <i>string</i>
Tree	failure-reason
Configurable	False
Platforms	Supported on all platforms

last-booted *string*

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
Context	platform control slot <i>string</i> last-booted <i>string</i>
Tree	last-booted
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-change *string*

Description	The date and time this component last changed state
Context	platform control slot <i>string</i> last-change <i>string</i>
Tree	last-change
String Length	20 to 32
Configurable	False

Platforms Supported on all platforms

locator-state *keyword*

Description Details if the locator LED is active on this component

Context [platform control slot](#) *string* [locator-state](#) *keyword*

Tree [locator-state](#)

Default inactive

Options

- active
Locator LED is currently active
- inactive
Locator LED is currently inactive

Configurable False

Platforms Supported on all platforms

manufactured-date *string*

Description The date this component was manufactured

Context [platform control slot](#) *string* [manufactured-date](#) *string*

Tree [manufactured-date](#)

Configurable False

Platforms Supported on all platforms

memory

Description Top-level container for system memory state

Context [platform control slot](#) *string* [memory](#)

Tree [memory](#)

Configurable False

Platforms Supported on all platforms

free *number*

Description Memory available for system use

Context [platform control slot](#) *string* [memory](#) [free](#) *number*

Tree [free](#)

Units	bytes
Configurable	False
Platforms	Supported on all platforms

physical number

Description	Total physical memory available on this component
Context	platform control slot <i>string</i> memory physical number
Tree	physical
Units	bytes
Configurable	False
Platforms	Supported on all platforms

reserved number

Description	Memory reserved for system use
Context	platform control slot <i>string</i> memory reserved number
Tree	reserved
Units	bytes
Configurable	False
Platforms	Supported on all platforms

utilization number

Description	Total memory utilized
Context	platform control slot <i>string</i> memory utilization number
Tree	utilization
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

oper-state keyword

Description	The operational state of this component
Context	platform control slot <i>string</i> oper-state keyword
Tree	oper-state

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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

part-number *string*

Description	Part number for this component
Context	platform control slot <i>string</i> part-number <i>string</i>
Tree	part-number
Configurable	False
Platforms	Supported on all platforms

power

Description	State related to power consumption and allocation for this component
Context	platform control slot <i>string</i> power
Tree	power
Configurable	False
Platforms	Supported on all platforms

allocated-power *number*

Description	The power budget allocated to this component
Context	platform control slot <i>string</i> power allocated-power <i>number</i>
Tree	allocated-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used-power *number*

Description	The power in use by this component
Context	platform control slot <i>string</i> power used-power <i>number</i>
Tree	used-power
Units	watts
Configurable	False
Platforms	Supported on all platforms

process [pid](#) *number*

Description	List of system processes
--------------------	--------------------------

Context	platform control slot <i>string</i> process pid <i>number</i>
Tree	process
Configurable	False
Platforms	Supported on all platforms

pid *number*

Description	The process ID
Context	platform control slot <i>string</i> process pid <i>number</i>
Configurable	False
Platforms	Supported on all platforms

args *string*

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.
Context	platform control slot <i>string</i> process pid <i>number</i> args <i>string</i>
Tree	args
Configurable	False
Platforms	Supported on all platforms

cpu-utilization *number*

Description	The percentage of CPU that is being used by the process
Context	platform control slot <i>string</i> process pid <i>number</i> cpu-utilization <i>number</i>
Tree	cpu-utilization
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

memory-usage *number*

Description	Kilobytes allocated and still in use by the process
Context	platform control slot <i>string</i> process pid <i>number</i> memory-usage <i>number</i>
Tree	memory-usage

Units	kilobytes
Configurable	False
Platforms	Supported on all platforms

memory-utilization *number*

Description	The percentage of RAM that is being used by the process
Context	platform control slot string process pid number memory-utilization number
Tree	memory-utilization
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

name *string*

Description	The process name
Context	platform control slot string process pid number name string
Tree	name
Configurable	False
Platforms	Supported on all platforms

start-time *string*

Description	The time at which this process started
Context	platform control slot string process pid number start-time string
Tree	start-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

removable *boolean*

Description	Details if this component can be removed from the system
Context	platform control slot string removable boolean
Tree	removable
Configurable	False

Platforms Supported on all platforms

role *keyword*

Description Control module role, detailing active or standby state
This field is not present on systems without removable control modules.

Context [platform control slot string role keyword](#)

Tree [role](#)

Options

- active
- standby

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

serial-number *string*

Description The serial number for this component

Context [platform control slot string serial-number string](#)

Tree [serial-number](#)

Configurable False

Platforms Supported on all platforms

software-version *string*

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.

Context [platform control slot string software-version string](#)

Tree [software-version](#)

Configurable False

Platforms Supported on all platforms

temperature

Description State related to temperature for this component

Context [platform control slot string temperature](#)

Tree [temperature](#)

Configurable	False
Platforms	Supported on all platforms

alarm-status *boolean*

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.
Context	platform control slot <i>string</i> temperature alarm-status <i>boolean</i>
Tree	alarm-status
Configurable	False
Platforms	Supported on all platforms

instant *number*

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.
Context	platform control slot <i>string</i> temperature instant <i>number</i>
Tree	instant
Configurable	False
Platforms	Supported on all platforms

margin *number*

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.
Context	platform control slot <i>string</i> temperature margin <i>number</i>
Tree	margin
Configurable	False
Platforms	Supported on all platforms

type *string*

Description	Control module type, as translated from the components EEPROM
Context	platform control slot string type string
Tree	type
Configurable	False
Platforms	Supported on all platforms

fabric slot *number*

Description	Top-level container for fabric configuration and state
Context	platform fabric slot number
Tree	fabric
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

slot *number*

Description	Numeric identifier for the fabric module
Context	platform fabric slot number
Range	1 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

admin-state *keyword*

Description	The administrative state of this component
Context	platform fabric slot number admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

clei-code *string*

Description	The Common Language Identification Code for this component
Context	platform fabric slot number clei-code string
Tree	clei-code
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

failure-reason *string*

Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Context	platform fabric slot number failure-reason string
Tree	failure-reason
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-booted *string*

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
Context	platform fabric slot number last-booted string
Tree	last-booted
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

last-change *string*

Description	The date and time this component last changed state
Context	platform fabric slot number last-change string
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

locator-state *keyword*

Description	Details if the locator LED is active on this component
Context	platform fabric slot number locator-state keyword
Tree	locator-state
Default	inactive
Options	<ul style="list-style-type: none"> • active Locator LED is currently active • inactive Locator LED is currently inactive
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

manufactured-date *string*

Description	The date this component was manufactured
Context	platform fabric slot number manufactured-date string
Tree	manufactured-date
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

oper-state *keyword*

Description	The operational state of this component
Context	platform fabric slot number oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

part-number *string*

Description	Part number for this component
Context	platform fabric slot number part-number string
Tree	part-number
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

power

Description	State related to power consumption and allocation for this component
Context	platform fabric slot number power

Tree	power
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

allocated-power *number*

Description	The power budget allocated to this component
Context	platform fabric slot number power allocated-power number
Tree	allocated-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used-power *number*

Description	The power in use by this component
Context	platform fabric slot number power used-power number
Tree	used-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

removable *boolean*

Description	Details if this component can be removed from the system
Context	platform fabric slot number removable boolean
Tree	removable
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

serial-number *string*

Description	The serial number for this component
Context	platform fabric slot number serial-number string
Tree	serial-number
Configurable	False

Platforms 7250 IXR-10, 7250 IXR-6

temperature

Description State related to temperature for this component

Context [platform fabric slot number temperature](#)

Tree [temperature](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

alarm-status *boolean*

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.

Context [platform fabric slot number temperature alarm-status boolean](#)

Tree [alarm-status](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

instant *number*

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.

Context [platform fabric slot number temperature instant number](#)

Tree [instant](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

margin *number*

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.

Context	platform fabric slot number temperature margin number
Tree	margin
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

type string

Description	Fabric module type, as translated from the components EEPROM
Context	platform fabric slot number type string
Tree	type
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

fan-tray id number

Description	Top-level container for fan module configuration and state
Context	platform fan-tray id number
Tree	fan-tray
Configurable	False
Platforms	Supported on all platforms

id number

Description	Numeric identifier for the fan tray
Context	platform fan-tray id number
Range	1 to 255
Configurable	False
Platforms	Supported on all platforms

clei-code string

Description	The Common Language Identification Code for this component
Context	platform fan-tray id number clei-code string
Tree	clei-code
Configurable	False

Platforms Supported on all platforms

failure-reason *string*

Description The reason the component transitioned to a failed state
Field is empty if the component is not currently in a failure state

Context [platform fan-tray id](#) *number* [failure-reason](#) *string*

Tree [failure-reason](#)

Configurable False

Platforms Supported on all platforms

last-booted *string*

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

Context [platform fan-tray id](#) *number* [last-booted](#) *string*

Tree [last-booted](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

last-change *string*

Description The date and time this component last changed state

Context [platform fan-tray id](#) *number* [last-change](#) *string*

Tree [last-change](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

locator-state *keyword*

Description Details if the locator LED is active on this component

Context [platform fan-tray id](#) *number* [locator-state](#) *keyword*

Tree [locator-state](#)

Default	inactive
Options	<ul style="list-style-type: none"> • active Locator LED is currently active • inactive Locator LED is currently inactive
Configurable	False
Platforms	Supported on all platforms

manufactured-date *string*

Description	The date this component was manufactured
Context	platform fan-tray id <i>number</i> manufactured-date <i>string</i>
Tree	manufactured-date
Configurable	False
Platforms	Supported on all platforms

oper-reason *keyword*

Description	Indicates the reason for the current state of this fan tray
Context	platform fan-tray id <i>number</i> oper-reason <i>keyword</i>
Tree	oper-reason
Options	<ul style="list-style-type: none"> • fault Hardware fault detected • eeprom-invalid EEPROM of this fan tray is either invalid or corrupt • airflow-mismatch The detected airflow of this fan tray does not match the system-calculated airflow direction The detected airflow of this fan tray does not match the system-calculated airflow direction The logic for determining the system-calculated direction is: - Majority wins between present fan trays - In the case where there are equal F2B or B2F fan-trays, PSUs are used as a tie break (PSUs only are counted in the event a tie breaker is needed) - F2B wins if no tie break can be used
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of this component
Context	platform fan-tray id <i>number</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the <code>reinvoke-with-delay</code> action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

part-number *string*

Description	Part number for this component
Context	platform fan-tray id number part-number string
Tree	part-number
Configurable	False
Platforms	Supported on all platforms

power

Description	State related to power consumption and allocation for this component
Context	platform fan-tray id number power
Tree	power
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

allocated-power *number*

Description	The power budget allocated to this component
Context	platform fan-tray id number power allocated-power number
Tree	allocated-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used-power *number*

Description	The power in use by this component
Context	platform fan-tray id number power used-power number
Tree	used-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

removable *boolean*

Description	Details if this component can be removed from the system
Context	platform fan-tray id <i>number</i> removable <i>boolean</i>
Tree	removable
Configurable	False
Platforms	Supported on all platforms

serial-number *string*

Description	The serial number for this component
Context	platform fan-tray id <i>number</i> serial-number <i>string</i>
Tree	serial-number
Configurable	False
Platforms	Supported on all platforms

speed *number*

Description	The current speed of the fan tray
Context	platform fan-tray id <i>number</i> speed <i>number</i>
Tree	speed
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

type *string*

Description	Fan tray type, as translated from the components EEPROM
Context	platform fan-tray id <i>number</i> type <i>string</i>
Tree	type
Configurable	False
Platforms	Supported on all platforms

linecard [slot](#) *number*

Description	Top-level container for linecard configuration and state
--------------------	--

Context	platform linecard slot number
Tree	linecard
Configurable	True
Platforms	Supported on all platforms

slot number

Description	Numeric identifier for the linecard
Context	platform linecard slot number
Range	1 to 8
Configurable	True
Platforms	Supported on all platforms

admin-state keyword

Description	The administrative state of this component
Context	platform linecard slot number admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

clei-code string

Description	The Common Language Identification Code for this component
Context	platform linecard slot number clei-code string
Tree	clei-code
Configurable	False
Platforms	Supported on all platforms

failure-reason string

Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
--------------------	--

Context	platform linecard slot number failure-reason string
Tree	failure-reason
Configurable	False
Platforms	Supported on all platforms

forwarding-complex [name keyword](#)

Description	List of forwarding complexes on the linecard
Context	platform linecard slot number forwarding-complex name keyword
Tree	forwarding-complex
Configurable	True
Platforms	Supported on all platforms

name [keyword](#)

Description	The identifier of the forwarding complex
Context	platform linecard slot number forwarding-complex name keyword
Options	<ul style="list-style-type: none"> • 0 • 1
Configurable	True
Platforms	Supported on all platforms

acl

Description	Enter the acl context
Context	platform linecard slot number forwarding-complex name keyword acl
Tree	acl
Configurable	False
Platforms	Supported on all platforms

resource [name identityref](#)

Description	Enter the resource list instance
Context	platform linecard slot number forwarding-complex name keyword acl resource name identityref
Tree	resource
Configurable	False

Platforms Supported on all platforms

name *identityref*

Description The name of the ACL resource

Context [platform](#) [linecard](#) [slot](#) *number* [forwarding-complex](#) [name](#) *keyword* [acl](#)
[resource](#) [name](#) *identityref*

Options

- [input-ipv4-filter-instances](#)

This 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-ipv4-filter-instances-routed](#)

This resource is used every time an IPv4 filter instance is created and applied to ingress traffic on routed subinterfaces. 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 routed subinterface using the IPv4 filter.

- [input-ipv4-filter-instances-bridged](#)

This resource is used every time an IPv4 filter instance is created and applied to ingress traffic on bridged subinterfaces. 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 bridged subinterface using the IPv4 filter.

- [input-ipv6-filter-instances](#)

This 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.

- [input-ipv6-filter-instances-routed](#)

This resource is used every time an IPv6 filter instance is created and applied to ingress traffic on routed subinterfaces. 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 routed subinterface using the IPv6 filter.

- [input-ipv6-filter-instances-bridged](#)

This resource is used every time an IPv6 filter instance is created and applied to ingress traffic on bridged subinterfaces. 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 bridged subinterface using the IPv6 filter.

- [if-input-ipv4-stats](#)

Resource pool of stats entries available for ingress IPv4 ACLs

- [if-input-ipv6-stats](#)

	Resource pool of stats entries available for ingress IPv6 ACLs
	<ul style="list-style-type: none"> • if-output-ipv4-stats
	Resource pool of stats entries available for egress IPv4 ACLs
	<ul style="list-style-type: none"> • if-output-ipv6-stats
	Resource pool of stats entries available for egress IPv6 ACLs
Configurable	False
Platforms	Supported on all platforms
free number	
Description	The number of resources that are unused and available
Context	platform linecard slot number forwarding-complex name keyword acl resource name identityref free number
Tree	free
Configurable	False
Platforms	Supported on all platforms
used number	
Description	The number of resources that are in use
Context	platform linecard slot number forwarding-complex name keyword acl resource name identityref used number
Tree	used
Configurable	False
Platforms	Supported on all platforms
buffer-memory	
Description	Container for utilization statistics of the packet buffer memory
Context	platform linecard slot number forwarding-complex name keyword buffer-memory
Tree	buffer-memory
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

dram

Description	Container for utilization statistics of the DRAM memory.
Context	platform linecard slot number forwarding-complex name keyword buffer-memory dram
Tree	dram
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	Used DRAM memory
Context	platform linecard slot number forwarding-complex name keyword buffer-memory dram used number
Tree	used
Range	0 to 100
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

free number

Description	Available buffer memory, which equals the total memory less the used memory and the reserved memory.
Context	platform linecard slot number forwarding-complex name keyword buffer-memory free number
Tree	free
Units	bytes
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

reserved number

Description	Reserved for internal purposes.
Context	platform linecard slot number forwarding-complex name keyword buffer-memory reserved number
Tree	reserved
Units	bytes
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

sram

Description Container for utilization statistics of the on-chip SRAM memory.

Context [platform linecard slot number forwarding-complex name keyword buffer-memory sram](#)

Tree [sram](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

free number

Description Available SRAM memory

Context [platform linecard slot number forwarding-complex name keyword buffer-memory sram free number](#)

Tree [free](#)

Units bytes

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

used number

Description Used SRAM memory

Context [platform linecard slot number forwarding-complex name keyword buffer-memory sram used number](#)

Tree [used](#)

Units bytes

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

used number

Description Used buffer memory, excluding reserved memory.

Context [platform linecard slot number forwarding-complex name keyword buffer-memory used number](#)

Tree [used](#)

Units	bytes
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D3

datapath

Description	Container for monitoring datapath resources of a particular forwarding complex
Context	platform linecard slot number forwarding-complex name keyword datapath
Tree	datapath
Configurable	False
Platforms	Supported on all platforms

asic

Description	Container for monitoring ASIC-specific datapath resources
Context	platform linecard slot number forwarding-complex name keyword datapath asic
Tree	asic
Configurable	False
Platforms	Supported on all platforms

resource [name identityref](#)

Description	List of ASIC-specific datapath resources.
Context	platform linecard slot number forwarding-complex name keyword datapath asic resource name identityref
Tree	resource
Configurable	False
Platforms	Supported on all platforms

name [identityref](#)

Description	The name of the ASIC-specific datapath resource
Context	platform linecard slot number forwarding-complex name keyword datapath asic resource name identityref
Options	<ul style="list-style-type: none"> ip-lpm-ipv4-routes

Trident3: Reports the number of IPv4 entries in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of half-wide entries in all partitions (i.e. it assumes no IPv6 routes consume those entries). In ALPM mode, free entries is the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv4 entries in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of half-wide entries in all partitions (i.e. it assumes no IPv6 routes consume those entries). In ALPM mode, free entries is the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv4 routes installed in the FIB. Free entries is the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv4 entries in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of half-wide entries in all partitions (i.e. it assumes no IPv6 routes consume those entries). In ALPM mode, free entries is the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv4 routes installed in the FIB. Free entries is the Minimum Guaranteed Capacity returned by the BCM SDK. Monterey: Reports the number of IPv4 routes installed in the FIB. Free entries is the Minimum Guaranteed Capacity returned by the BCM SDK.

- ip-lpm-ipv6-shorter-routes

Trident3: Reports the number of IPv6 entries with prefix length less than 65 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of single-wide + double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length less than 65 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of single-wide + double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv6 entries with prefix length less than 65 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length less than 65 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of single-wide + double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv6 entries with prefix length less than 65 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Monterey: Reports the number of IPv6 entries with prefix length less than 65 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

- ip-lpm-ipv6-longer-routes

Trident3: Reports the number of IPv6 entries with prefix length greater than 64 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length greater than 64 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Tomahawk3: Reports the number of IPv6 entries with prefix length greater than 64 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length greater than 64 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Tomahawk3: Reports the number of IPv6 entries with prefix length greater than 64 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Monterey: Reports the number of IPv6 entries with prefix length greater than 64 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

- exact-match-entries

Reports the number of half-wide entries used in the LEM table. Each MPLS ILM record uses one half-wide entry. Each IPv4 address used as a host route, ARP entry or subnet broadcast address requires a half-wide entry. An IPv6 address used as a host route, or ND entry requires a single-wide entry (2 half-wide entries). Free entries is the remaining number of half-wide entries.

- underlay-ecmp-groups

Underlay ECMP group resources.

Underlay ECMP group resources. ECMP groups are partitioned into overlay and underlay groups. The underlay partition is further subdivided into groups used for underlay ECMP and groups used for VP LAGs (EVPN M-H). This counts the utilization of the sub-resource used for ECMP.

- vp-lag-groups

VP LAG group resources.

VP LAG group resources. ECMP groups are partitioned into overlay and underlay groups. The underlay partition is further subdivided into groups used for underlay ECMP and groups used for VP LAGs (EVPN M-H). This counts the utilization of the sub-resource used for VP LAGs.

- overlay-ecmp-groups

Overlay ECMP group resources.

Overlay ECMP group resources. ECMP groups are partitioned into overlay and underlay groups. This counts the utilization of the overlay ECMP partition.

- underlay-ecmp-members

Underlay ECMP member resources.

Underlay ECMP member resources. ECMP members are partitioned into overlay and underlay. This counts the utilization of the partition used for underlay.

- overlay-ecmp-members

Overlay ECMP member resources.

Overlay ECMP member resources. ECMP members are partitioned into overlay and underlay. This counts the utilization of the partition used for overlay.

- underlay-egress-next-hops

Underlay egress next-hop resources.

Underlay egress next-hop resources. Egress next-hops are partitioned into overlay and underlay. This counts the utilization of the partition used for underlay.

- overlay-egress-next-hops

Overlay egress next-hop resources.

Overlay egress next-hop resources. Egress next-hops are partitioned into overlay and underlay. This counts the utilization of the partition used for overlay.

- dgpp-module-ids

DGPP module ID resources.

DGPP module ID resources. DGPPs are an aggregate id consisting of a module_id and a port_id. There are 64 modules and 120 ports per module. Each 'network' ARP entry (IP next-hop) needs a DGPP - the module_id is allocated against the network interface (port) and a port_id is allocated from within the module. A module_id will only be allocated when the first ArpEntry is added (freed when last is removed) but is owned exclusively by that network interface. A network interface may require more than one module_id - i.e. if there are 245 ArpEntries on ethernet-1/1 (possibly spread across multiple network-instance interfaces) then 3 module_ids are required.

- egress-vlan-translate-egress-vnis

EGR_VLAN_XLATE_1 resources.

EGR_VLAN_XLATE_1 resources. Corresponds to the 'EGR_VLAN_XLATE_1' HW table (8K entries). These entries are used for finding the egress VNI to be used for VXLAN packets.

- egress-vlan-translate-local-bias-pairs

EGR_VLAN_XLATE_2 resources.

EGR_VLAN_XLATE_2 resources. Corresponds to the 'EGR_VLAN_XLATE_2' HW table (24K entries). These entries are used for local bias (ES pruning).

- level-1-ecmp-groups

L1 ECMP group resources.

L1 ECMP group resources. ECMP FEC resources are divided into L1 ECMP FEC resources and L2 ECMP FEC resources. This counts the number of entries used in the L1 partition.

- level-2-ecmp-groups

L2 ECMP group resources.

L2 ECMP group resources. ECMP FEC resources are divided into L1 ECMP FEC resources and L2 ECMP FEC resources. This counts the number of entries used in the L2 partition.

- level-1-ecmp-members

L1 ECMP member resources.

L1 ECMP member resources. ECMP FEC member resources are divided into L1 and L2 resources. This counts the number of entries used in the L1 partition.

- level-2-ecmp-members

L2 ECMP member resources.

L2 ECMP member resources. ECMP FEC member resources are divided into L1 and L2 resources. This counts the number of entries used in the L2 partition.

- level-1-non-ecmp-fecs

L1 non-ECMP FEC resources.

L1 non-ECMP FEC resources. Non-ECMP FEC resources are divided into L1 and L2 resources. This counts the number of entries used in the L1 partition.

- level-2-non-ecmp-fecs

L2 non-ECMP FEC resources.

L2 non-ECMP FEC resources. Non-ECMP FEC resources are divided into L1 and L2 resources. This counts the number of entries used in the L2 partition.

Configurable

False

Platforms

Supported on all platforms

free-entries *number*

Description

The number of entries that are currently free

Context

[platform](#) [linecard](#) [slot](#) [number](#) [forwarding-complex](#) [name](#) [keyword](#) [datapath](#)
[asic](#) [resource](#) [name](#) [identityref](#) [free-entries](#) [number](#)

Tree	free-entries
Configurable	False
Platforms	Supported on all platforms

used-entries *number*

Description	The number of entries that are currently used
Context	platform linecard slot number forwarding-complex name keyword datapath asic resource name identityref used-entries number
Tree	used-entries
Configurable	False
Platforms	Supported on all platforms

used-percent *number*

Description	The percentage of the resource that is currently used
Context	platform linecard slot number forwarding-complex name keyword datapath asic resource name identityref used-percent number
Tree	used-percent
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

xdp

Description	Container for monitoring datapath resources that are generic in concept.
Context	platform linecard slot number forwarding-complex name keyword datapath xdp
Tree	xdp
Configurable	False
Platforms	Supported on all platforms

resource [name](#) *identityref*

Description	List of generic datapath resources.
Context	platform linecard slot number forwarding-complex name keyword datapath xdp resource name identityref
Tree	resource

Configurable	False
Platforms	Supported on all platforms

name *identityref*

Description	The name of the XDP datapath resource
Context	platform linecard slot number forwarding-complex name keyword datapath xdp resource name identityref
Options	<ul style="list-style-type: none"> arp-nd-entries <p>IPv4 ARP and IPv6 neighbor discovery resources.</p> <p>IPv4 ARP and IPv6 neighbor discovery resources. Each IPv4 ARP and each IPv6 neighbor entry counts as 1 used resource against a total that is platform dependent. This does not consider underlying ASIC resources.</p> ip-hosts <p>IP host route resources.</p> <p>IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks</p> <p>IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks Tomahawk3: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries.</p> <p>IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks Tomahawk3: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries. Monterey: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries.</p> ip-lpm-routes

IP longest prefix match route resources.

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes.

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes. Trident3 and Tomahawk3: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route (or index to IPv4 ALPM lookup) requires a half-wide entry. An IPv6 route (or index to IPv6 ALPM lookup) that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route (or index to IPv6 ALPM lookup) that is more than /64 requires a double-wide entry (4 half-wide entries).

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes. Trident3 and Tomahawk3: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route (or index to IPv4 ALPM lookup) requires a half-wide entry. An IPv6 route (or index to IPv6 ALPM lookup) that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route (or index to IPv6 ALPM lookup) that is more than /64 requires a double-wide entry (4 half-wide entries). Monterey: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route requires a half-wide entry. An IPv6 route that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route that is more than /64 requires a double-wide entry (4 half-wide entries).

- mac-addresses

MAC address resources.

MAC address resources. Reports the used number of entries, where 1 entry = 1 MAC address. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks

- direct-next-hops

Direct next-hop resources.

Direct next-hop resources. Reports the number of entries, where 1 entry is used for every next-hop of an IP or MPLS route that is resolved directly to a local interface. This does not consider underlying ASIC resources.

- indirect-next-hops

Indirect next-hop resources.

Indirect next-hop resources. Reports the number of entries, where 1 entry is used for every next-hop of an IP route that is resolved by a non-local route. This does not consider underlying ASIC resources.

- tunnel-next-hops

Tunnel next-hop resources.

Tunnel next-hop resources. Reports the number of tunnel next-hop entries. For EVPN routes resolved by VXLAN, 1 entry is used for every

<vni, vtep> pair. When a BGP IP route is resolved by an MPLS tunnel, 1 entry is used for every BGP next-hop of the route. This does not consider underlying ASIC resources.

- **ecmp-groups**

ECMP group resources.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups. Tomahawk3: Reports used number of ECMP groups.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups. Tomahawk3: Reports used number of ECMP groups. Monterey: Reports used number of ECMP groups.

- **ecmp-members**

ECMP member resources.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members. Tomahawk3: Reports used number of ECMP members.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members. Tomahawk3: Reports used number of ECMP members. Monterey: Reports used number of ECMP members.

- **egress-next-hops**

Egress next-hop resources.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Tomahawk3: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Tomahawk3: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Monterey: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

- lag-groups

LAG group resources.

LAG group resources. Reports the number of LAG resources used, including DGPP LAGs.

- lag-members

LAG member resources.

LAG member resources. Reports the number of LAG member resources used, including DGPP LAG members.

- subinterfaces

Subinterface resources.

Subinterface resources. There are a maximum of 127 subinterfaces per TH3 pipeline (limited by VFP/EFP TCAM resources). This counts the utilization of those resources.

- mpls-next-hops

One resource is used for every next-hop that pushes an MPLS label in every next-hop-group that is tied to an ILM entry that performs a 'swap'. One additional resource is used for every next-hop that pushes an MPLS label in every next-hop-group that is tied to an MPLS tunnel.

- mpls-incoming-labels

One resource is used for every MPLS ILM entry that performs either a 'swap' or a 'pop' operation.

- tunnels

Tunnel resources. One tunnel resource is used per VXLAN or MPLS tunnel endpoint.

Tunnel resources. One tunnel resource is used per VXLAN or MPLS tunnel endpoint. On TD3 systems this equates to a DVP resource.

Configurable

False

Platforms

Supported on all platforms

free-entries *number*

Description	The number of entries that are currently free
Context	platform linecard slot number forwarding-complex name keyword datapath xdp resource name identityref free-entries number
Tree	free-entries
Configurable	False
Platforms	Supported on all platforms

used-entries *number*

Description	The number of entries that are currently used
Context	platform linecard slot number forwarding-complex name keyword datapath xdp resource name identityref used-entries number
Tree	used-entries
Configurable	False
Platforms	Supported on all platforms

used-percent *number*

Description	The percentage of the resource that is currently used
Context	platform linecard slot number forwarding-complex name keyword datapath xdp resource name identityref used-percent number
Tree	used-percent
Range	0 to 100
Configurable	False
Platforms	Supported on all platforms

fabric

Description	Top-level container for fabric configuration and state
Context	platform linecard slot number forwarding-complex name keyword fabric
Tree	fabric
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

availability number

Description	Details the percentage bandwidth available to the fabric for the line card
Context	platform linecard slot number forwarding-complex name keyword fabric availability number
Tree	availability
Range	0 to 100
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

utilization-egress number

Description	Provides the linecard bandwidth utilization from the switch fabric
Context	platform linecard slot number forwarding-complex name keyword fabric utilization-egress number
Tree	utilization-egress
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

utilization-ingress number

Description	Provides the linecard bandwidth utilization into the switch fabric
Context	platform linecard slot number forwarding-complex name keyword fabric utilization-ingress number
Tree	utilization-ingress
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

mtu

Description	Enter the mtu context
Context	platform linecard slot number forwarding-complex name keyword mtu
Tree	mtu
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

resource name *identityref*

Description	Enter the resource list instance
Context	platform linecard slot number forwarding-complex name keyword mtu resource name identityref
Tree	resource
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

name *identityref*

Description	The name of the MTU resource
Context	platform linecard slot number forwarding-complex name keyword mtu resource name identityref
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. • mpls-mtu MPLS MTU resource pool. One resource from this pool is consumed by every different MPLS MTU value used by the subinterfaces on the linecard forwarding-complex.
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

free *number*

Description	The number of resources that are unused and available
Context	platform linecard slot number forwarding-complex name keyword mtu resource name identityref free number
Tree	free
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	The number of resources that are in use
Context	platform linecard slot number forwarding-complex name keyword mtu resource name identityref used number
Tree	used
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

pipeline index (*number | keyword*)

Description	List of pipelines that make up one forwarding complex.
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword)
Tree	pipeline
Configurable	True
Platforms	7220 IXR-H3, 7220 IXR-H2

index (*number | keyword*)

Description	The pipeline number (TH3 systems) or direction (J2 and J2C+ systems).
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword)
Range	0 to 7
Options	<ul style="list-style-type: none"> • egress Applicable to J2 and J2C+ systems only • ingress Applicable to J2 and J2C+ systems only
Configurable	True
Platforms	7220 IXR-H3, 7220 IXR-H2

datapath

Description	Container for monitoring datapath resources of a particular pipeline
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) datapath
Tree	datapath
Configurable	False

Platforms 7220 IXR-H3, 7220 IXR-H2

xdp

Description Container for monitoring datapath resources that are generic in concept. At the pipeline level only one XDP resource is currently reported:

Context [platform linecard slot number forwarding-complex name keyword pipeline index \(number | keyword\) datapath xdp](#)

Tree [xdp](#)

Configurable False

Platforms 7220 IXR-H3, 7220 IXR-H2

resource [name identityref](#)

Description List of generic datapath resources.

Context [platform linecard slot number forwarding-complex name keyword pipeline index \(number | keyword\) datapath xdp resource name identityref](#)

Tree [resource](#)

Configurable False

Platforms 7220 IXR-H3, 7220 IXR-H2

name [identityref](#)

Description The name of the XDP datapath resource

Context [platform linecard slot number forwarding-complex name keyword pipeline index \(number | keyword\) datapath xdp resource name identityref](#)

Options

- arp-nd-entries

IPv4 ARP and IPv6 neighbor discovery resources.

IPv4 ARP and IPv6 neighbor discovery resources. Each IPv4 ARP and each IPv6 neighbor entry counts as 1 used resource against a total that is platform dependent. This does not consider underlying ASIC resources.
- ip-hosts

IP host route resources.

IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks

IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks Tomahawk3: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries.

IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks Tomahawk3: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries. Monterey: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries.

- ip-lpm-routes

IP longest prefix match route resources.

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes.

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes. Trident3 and Tomahawk3: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route (or index to IPv4 ALPM lookup) requires a half-wide entry. An IPv6 route (or index to IPv6 ALPM lookup) that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route (or index to IPv6 ALPM lookup) that is more than /64 requires a double-wide entry (4 half-wide entries).

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes. Trident3 and Tomahawk3: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route (or index to IPv4 ALPM lookup) requires a half-wide entry. An IPv6 route (or index to IPv6 ALPM lookup) that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route (or index to IPv6 ALPM lookup) that is more than /64 requires a double-wide entry (4 half-wide entries). Monterey: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route requires a half-wide entry. An IPv6 route that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route that is more than /64 requires a double-wide entry (4 half-wide entries).

- mac-addresses
MAC address resources.
MAC address resources. Reports the used number of entries, where 1 entry = 1 MAC address. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks
- direct-next-hops
Direct next-hop resources.
Direct next-hop resources. Reports the number of entries, where 1 entry is used for every next-hop of an IP or MPLS route that is resolved directly to a local interface. This does not consider underlying ASIC resources.
- indirect-next-hops
Indirect next-hop resources.
Indirect next-hop resources. Reports the number of entries, where 1 entry is used for every next-hop of an IP route that is resolved by a non-local route. This does not consider underlying ASIC resources.
- tunnel-next-hops
Tunnel next-hop resources.
Tunnel next-hop resources. Reports the number of tunnel next-hop entries. For EVPN routes resolved by VXLAN, 1 entry is used for every <vni, vtep> pair. When a BGP IP route is resolved by an MPLS tunnel, 1 entry is used for every BGP next-hop of the route. This does not consider underlying ASIC resources.
- ecmp-groups
ECMP group resources.
ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs.
ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups.
ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups. Tomahawk3: Reports used number of ECMP groups.
ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups. Tomahawk3: Reports used number of ECMP groups. Monterey: Reports used number of ECMP groups.
- ecmp-members
ECMP member resources.
ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members. Tomahawk3: Reports used number of ECMP members.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members. Tomahawk3: Reports used number of ECMP members. Monterey: Reports used number of ECMP members.

- egress-next-hops

Egress next-hop resources.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Tomahawk3: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Tomahawk3: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Monterey: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

- lag-groups

LAG group resources.

LAG group resources. Reports the number of LAG resources used, including DGPP LAGs.

- lag-members

LAG member resources.

LAG member resources. Reports the number of LAG member resources used, including DGPP LAG members.

- subinterfaces

Subinterface resources.

Subinterface resources. There are a maximum of 127 subinterfaces per TH3 pipeline (limited by VFP/EFP TCAM resources). This counts the utilization of those resources.

- **mpls-next-hops**

One resource is used for every next-hop that pushes an MPLS label in every next-hop-group that is tied to an ILM entry that performs a 'swap'. One additional resource is used for every next-hop that pushes an MPLS label in every next-hop-group that is tied to an MPLS tunnel.

- **mpls-incoming-labels**

One resource is used for every MPLS ILM entry that performs either a 'swap' or a 'pop' operation.

- **tunnels**

Tunnel resources. One tunnel resource is used per VXLAN or MPLS tunnel endpoint.

Tunnel resources. One tunnel resource is used per VXLAN or MPLS tunnel endpoint. On TD3 systems this equates to a DVP resource.

Configurable	False
Platforms	7220 IXR-H3, 7220 IXR-H2

free-entries *number*

Description	The number of entries that are currently free
Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> pipeline index (<i>number</i> <i>keyword</i>) datapath xdp resource name <i>identityref</i> free-entries <i>number</i>
Tree	free-entries
Configurable	False
Platforms	7220 IXR-H3, 7220 IXR-H2

used-entries *number*

Description	The number of entries that are currently used
Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> pipeline index (<i>number</i> <i>keyword</i>) datapath xdp resource name <i>identityref</i> used-entries <i>number</i>
Tree	used-entries
Configurable	False
Platforms	7220 IXR-H3, 7220 IXR-H2

used-percent *number*

Description	The percentage of the resource that is currently used
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) datapath xdp resource name identityref used-percent number
Tree	used-percent
Range	0 to 100
Configurable	False
Platforms	7220 IXR-H3, 7220 IXR-H2

pipeline-counters

Description	Top-level container for the packet counters associated with the different NPU sub-blocks.
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters
Tree	pipeline-counters
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

host-interface-block

Description	The ASIC host interface block subsystem that connects the NPU to the host CPU (on the CPM)
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block
Tree	host-interface-block
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

packet-extraction

Description	Packet extraction from the NPU towards the CPU
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction
Tree	packet-extraction
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

extracted-octets *number*

Description	The number of octets in Ethernet frames extracted towards the CPU from the pipeline; this includes packets that might be dropped (due to congestion or rate limiting) before reaching the final consuming application on the CPM
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction extracted-octets number
Tree	extracted-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

extracted-packets *number*

Description	The number of Ethernet frames extracted towards the CPU from the pipeline; this includes packets that might be dropped (due to congestion or rate limiting) before reaching the final consuming application on the CPM
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction extracted-packets number
Tree	extracted-packets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

extraction-reason [reason](#) *identityref*

Description	List of extraction reasons that are possible for the pipeline
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction extraction-reason reason identityref
Tree	extraction-reason
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

reason *identityref*

Description	A reason for extracting the packet towards the host CPU
--------------------	---

Context	platform linecard slot <i>number</i> forwarding-complex name <i>keyword</i> pipeline index (<i>number</i> <i>keyword</i>) pipeline-counters host-interface-block packet-extraction extraction-reason reason <i>identityref</i>
Options	<ul style="list-style-type: none"> • ipv4-header-options IPv4 header options are present in the packet. • ipv6-hop-by-hop-option IPv6 packet with topmost next-header value of zero. • icmp ICMPv4 packets with this router as destination. • icmp6 ICMPv6 packets including neighbor-solicitation and neighbor-advertisement messages. • icmp-redirect Received IPv4 and IPv6 packets that should cause an ICMP redirect to be generated. • bfd BFD and micro-BFD packets with this router as destination. • bgp BGP packets; TCP port 179. • grpc GRPC packets; TCP port 57400 • ospf OSPF packets; IP protocol 89 • vrrp VRRP packets; IP protocol 112 • ldp LDP packets; UDP port 646 • dhcp DHCP packets; UDP ports 67,68 • ip-other-terminating Any other IP packets that are locally destined • ip-blackhole-icmp Traffic matched a blackhole route with generate-icmp=true • ipv6-multicast IPv6 DA = FF01:0:0:0:0:0:1 or IPv6 DA = FF01:0:0:0:0:0:2 • ipv6-link-local IPv6 DA = FE80::/10 address • ipv4-broadcast

IPv4 packets were received with a subnet broadcast address or a limited broadcast and not recognized as another type

- ip-no-route

IPv4 and IPv6 packets for which there was no route to the destination

- ip-header-errors

IP version error, IP header checksum error, IP header length error, IP header total length error, IPv6 next-header is null, IPv6 SA is link-local while IPv6 DA is global

- ip-ttl-expired

The IP packet is not destined for this router and it was received with TTL 0 or TTL 1

- mpls-ttl-expired

The MPLS packet was received with MPLS label stack TTL 0 or TTL 1

- ip-arp-miss

The IP DA itself or the next-hop of the route used to forward the packet has no ARP/IPv6 neighbor entry

- ip-arp

The received frame is an ARP packet recognized by ethertype 0x0806

- lldp

The received frame is an LLDP packet recognized by ethertype 0x88cc

- isis

The received frame is an ISIS packet

- lacp

The received frame is an LACP packet

- google-discovery

The received frame is a GDP packet recognized by ethertype 0x6007

- capture-filter-copy

Packets matching a capture-filter copy rule

- cpm-filter-log

Packets matching a CPM-filter rule with log action

- ingress-acl-log

Packets matching an interface IP filter rule with log action

- egress-acl-log

Packet matched an egress ACL rule with log action.

- ip-mpls-mtu-exceeded

The egress subinterface IP MTU or MPLS MTU (as applicable) is less than the size of the IP or MPLS packet that needs to be transmitted.

Configurable

False

Platforms 7250 IXR-10, 7250 IXR-6

extracted-octets *number*

Description The number of octets in Ethernet frames extracted towards the CPU from the pipeline; this includes packets that might be dropped (due to congestion or rate limiting) before reaching the final consuming application on the CPM

Context [platform linecard slot number forwarding-complex name keyword pipeline index \(number | keyword\) pipeline-counters host-interface-block packet-extraction extraction-reason reason identityref extracted-octets number](#)

Tree [extracted-octets](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

extracted-packets *number*

Description The number of Ethernet frames extracted towards the CPU from the pipeline; this includes packets that might be dropped (due to congestion or rate limiting) before reaching the final consuming application on the CPM

Context [platform linecard slot number forwarding-complex name keyword pipeline index \(number | keyword\) pipeline-counters host-interface-block packet-extraction extraction-reason reason identityref extracted-packets number](#)

Tree [extracted-packets](#)

Default 0

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

forwarding-class *fc keyword*

Description Enter the forwarding-class list instance

Context [platform linecard slot number forwarding-complex name keyword pipeline index \(number | keyword\) pipeline-counters host-interface-block packet-extraction forwarding-class fc keyword](#)

Tree [forwarding-class](#)

Configurable False

Platforms 7250 IXR-10, 7250 IXR-6

fc keyword

Description	One of the forwarding classes
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction forwarding-class fc keyword
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

extracted-octets number

Description	The number of octets in Ethernet frames extracted towards the CPU from the pipeline; this includes packets that might be dropped (due to congestion or rate limiting) before reaching the final consuming application on the CPM
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction forwarding-class fc keyword extracted-octets number
Tree	extracted-octets
Default	0
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

extracted-packets number

Description	The number of Ethernet frames extracted towards the CPU from the pipeline; this includes packets that might be dropped (due to congestion or rate limiting) before reaching the final consuming application on the CPM
Context	platform linecard slot number forwarding-complex name keyword pipeline index (number keyword) pipeline-counters host-interface-block packet-extraction forwarding-class fc keyword extracted-packets number
Tree	extracted-packets
Default	0

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

qos

Description	Enter the qos context
Context	platform linecard slot number forwarding-complex name keyword qos
Tree	qos
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

resource name *identityref*

Description	Enter the resource list instance
Context	platform linecard slot number forwarding-complex name keyword qos resource name <i>identityref</i>
Tree	resource
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

name *identityref*

Description	The name of the QoS resource
Context	platform linecard slot number forwarding-complex name keyword qos resource name <i>identityref</i>
Options	<ul style="list-style-type: none"> • classifier-profiles <p>A classifier-profile resource is used every time a different combination of IPv4 DSCP classifier and IPv6 DSCP classifier is applied to an ingress subinterface of the 7250 IXR IMM. There are 16 of these resources and one is always used by the combination of the default IPv4 DSCP classifier and the default IPv6 DSCP classifier.</p> • rewrite-profiles <p>On the 7250 IXR, a rewrite-profile resource is used every time a different combination of IPv4 DSCP rewrite-rule and IPv6 DSCP rewrite-rule is applied to an egress subinterface of the 7250 IXR IMM. There are 32 of these resources.</p> <p>On the 7250 IXR, a rewrite-profile resource is used every time a different combination of IPv4 DSCP rewrite-rule and IPv6 DSCP rewrite-rule is applied to an egress subinterface of the 7250 IXR IMM. There are 32 of these resources. On the SAS, a rewrite-profile is used every time a different combination of dot1p and MPLS traffic-class rewrite-rule is</p>

applied to an egress subinterface of the system. There are 15 of these resources.

- rewrite-policies

A rewrite-policy resource is used every time a different DSCP or MPLS traffic-class rewrite-rule policy is applied to an egress subinterface of the 7250 IXR IMM. There are 32 of these resources.

Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

free number

Description	The number of resources that are unused and available
Context	platform linecard slot number forwarding-complex name keyword qos resource name identityref free number
Tree	free
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used number

Description	The number of resources that are in use
Context	platform linecard slot number forwarding-complex name keyword qos resource name identityref used number
Tree	used
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

tcam

Description	Enter the tcam context
Context	platform linecard slot number forwarding-complex name keyword tcam
Tree	tcam
Configurable	False
Platforms	Supported on all platforms

resource name identityref

Description	Enter the resource list instance
--------------------	----------------------------------

Context	platform linecard slot number forwarding-complex name keyword tcam resource name identityref
Tree	resource
Configurable	False
Platforms	Supported on all platforms

name *identityref*

Description	The name of the TCAM resource
Context	platform linecard slot number forwarding-complex name keyword tcam resource name identityref
Options	<ul style="list-style-type: none"> • if-input-ipv4 Resource pool of TCAM entries used by IPv4 ACLs applied as subinterface-input filters • if-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 • system-capture-ipv4 Resource pool of TCAM entries used by IPv4 capture-filter ACLs and IPv4 system-filter ACLs • system-capture-ipv6 Resource pool of TCAM entries used by IPv6 capture-filter ACLs and IPv6 system-filter ACLs • capture-ipv4 Resource pool of TCAM entries used by IPv4 capture-filter ACLs • capture-ipv6 Resource pool of TCAM entries used by IPv6 capture-filter ACLs • if-output-cpm-ipv4

- Resource pool of TCAM entries used by IPv4 egress ACLs and cpm-filter ACLs
- if-output-cpm-ipv6
 - Resource pool of TCAM entries used by IPv6 egress ACLs and cpm-filter ACLs
- if-input-mac
 - Resource pool of TCAM entries used by MAC ACLs applied as subinterface-input filters
- if-output-cpm-mac
 - Resource pool of TCAM entries used by MAC egress ACLs and MAC cpm-filter ACLs
- policy-forwarding-ipv4
 - Resource pool of TCAM entries used by IPv4 policy-forwarding entries

Configurable	False
Platforms	Supported on all platforms

free-dynamic *number*

Description	The number of available and unused TCAM entries for the entry type, assuming that all the remaining unused TCAM slices would be dynamically allocated to this one type of entry (subject to chip level constraints on the placement of double-wide and triple-wide TCAM slice groups).
Context	platform linecard slot number forwarding-complex name keyword tcam resource name identityref free-dynamic number
Tree	free-dynamic
Configurable	False
Platforms	Supported on all platforms

free-static *number*

Description	The number of available and unused TCAM entries for the entry type, assuming that the number of dynamic TCAM slices that are currently allocated to the entry type remains constant at its current value.
Context	platform linecard slot number forwarding-complex name keyword tcam resource name identityref free-static number
Tree	free-static
Configurable	False
Platforms	Supported on all platforms

programmed *number*

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.
Context	platform linecard slot number forwarding-complex name keyword tcam resource name identityref programmed number
Tree	programmed
Configurable	False
Platforms	Supported on all platforms

reserved *number*

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.
Context	platform linecard slot number forwarding-complex name keyword tcam resource name identityref reserved number
Tree	reserved
Configurable	False
Platforms	Supported on all platforms

last-booted *string*

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
Context	platform linecard slot number last-booted string
Tree	last-booted
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-change *string*

Description	The date and time this component last changed state
Context	platform linecard slot number last-change string
Tree	last-change

String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

locator-state *keyword*

Description	Details if the locator LED is active on this component
Context	platform linecard slot number locator-state keyword
Tree	locator-state
Default	inactive
Options	<ul style="list-style-type: none"> • active Locator LED is currently active • inactive Locator LED is currently inactive
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

manufactured-date *string*

Description	The date this component was manufactured
Context	platform linecard slot number manufactured-date string
Tree	manufactured-date
Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	The operational state of this component
Context	platform linecard slot number oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

part-number string**Description**

Part number for this component

Context[platform](#) [linecard slot](#) [number](#) [part-number string](#)**Tree**[part-number](#)**Configurable**

False

Platforms

Supported on all platforms

power

Description	State related to power consumption and allocation for this component
Context	platform linecard slot number power
Tree	power
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

allocated-power number

Description	The power budget allocated to this component
Context	platform linecard slot number power allocated-power number
Tree	allocated-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

used-power number

Description	The power in use by this component
Context	platform linecard slot number power used-power number
Tree	used-power
Units	watts
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

removable boolean

Description	Details if this component can be removed from the system
Context	platform linecard slot number removable boolean
Tree	removable
Configurable	False
Platforms	Supported on all platforms

serial-number string

Description	The serial number for this component
--------------------	--------------------------------------

Context	platform linecard slot number serial-number string
Tree	serial-number
Configurable	False
Platforms	Supported on all platforms

software-version *string*

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.
Context	platform linecard slot number software-version string
Tree	software-version
Configurable	False
Platforms	Supported on all platforms

temperature

Description	State related to temperature for this component
Context	platform linecard slot number temperature
Tree	temperature
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

alarm-status *boolean*

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.
Context	platform linecard slot number temperature alarm-status boolean
Tree	alarm-status
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

instant number

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.
Context	platform linecard slot number temperature instant number
Tree	instant
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

margin number

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.
Context	platform linecard slot number temperature margin number
Tree	margin
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

type string

Description	Linecard type, as translated from the components EEPROM
Context	platform linecard slot number type string
Tree	type
Configurable	False
Platforms	Supported on all platforms

power-supply id number

Description	Top-level container for power supply module configuration and state
Context	platform power-supply id number
Tree	power-supply
Configurable	False
Platforms	Supported on all platforms

id number

Description	Numeric identifier for the power supply module
Context	platform power-supply id number
Range	1 to 255
Configurable	False
Platforms	Supported on all platforms

capacity number

Description	The total capacity the power supply module can provide
Context	platform power-supply id number capacity number
Tree	capacity
Units	watts
Configurable	False
Platforms	Supported on all platforms

clei-code string

Description	The Common Language Identification Code for this component
Context	platform power-supply id number clei-code string
Tree	clei-code
Configurable	False
Platforms	Supported on all platforms

failure-reason string

Description	The reason the component transitioned to a failed state Field is empty if the component is not currently in a failure state
Context	platform power-supply id number failure-reason string
Tree	failure-reason
Configurable	False
Platforms	Supported on all platforms

input

Description	Top-level container for power-supply input state
Context	platform power-supply id number input
Tree	input
Configurable	False
Platforms	Supported on all platforms

current *decimal-number*

Description	Current input amperage for the power-supply
Context	platform power-supply id number input current decimal-number
Tree	current
Units	amps
Configurable	False
Platforms	Supported on all platforms

power *decimal-number*

Description	Current input power for the power-supply
Context	platform power-supply id number input power decimal-number
Tree	power
Units	watts
Configurable	False
Platforms	Supported on all platforms

voltage *decimal-number*

Description	Current input voltage for the power-supply
Context	platform power-supply id number input voltage decimal-number
Tree	voltage
Units	volts
Configurable	False
Platforms	Supported on all platforms

last-booted *string*

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
Context	platform power-supply id <i>number</i> last-booted <i>string</i>
Tree	last-booted
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-change *string*

Description	The date and time this component last changed state
Context	platform power-supply id <i>number</i> last-change <i>string</i>
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

manufactured-date *string*

Description	The date this component was manufactured
Context	platform power-supply id <i>number</i> manufactured-date <i>string</i>
Tree	manufactured-date
Configurable	False
Platforms	Supported on all platforms

oper-reason *keyword*

Description	Indicates the reason for the current state of the component
Context	platform power-supply id <i>number</i> oper-reason <i>keyword</i>
Tree	oper-reason
Options	<ul style="list-style-type: none"> no-input/fault No power input, or other hardware fault detected eeeprom-invalid EEPROM of this power supply is either invalid or corrupt

- **airflow-mismatch**
The detected airflow of this power supply does not match the system-calculated airflow direction
The detected airflow of this power supply does not match the system-calculated airflow direction The logic for determining the system-calculated direction is: - Majority wins between present fan trays - In the case where there are equal F2B or B2F fan-trays, PSUs are used as a tie break (PSUs only are counted in the event a tie breaker is needed) - F2B wins if no tie break can be used
- Configurable** False
- Platforms** Supported on all platforms

oper-state *keyword*

Description	The operational state of this component
Context	platform power-supply id number oper-state keyword
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state

- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

part-number *string*

Description	Part number for this component
Context	platform power-supply id <i>number</i> part-number <i>string</i>
Tree	part-number
Configurable	False
Platforms	Supported on all platforms

removable *boolean*

Description	Details if this component can be removed from the system
Context	platform power-supply id <i>number</i> removable <i>boolean</i>
Tree	removable
Configurable	False
Platforms	Supported on all platforms

serial-number *string*

Description	The serial number for this component
Context	platform power-supply id <i>number</i> serial-number <i>string</i>
Tree	serial-number
Configurable	False
Platforms	Supported on all platforms

temperature

Description	State related to temperature for this component
Context	platform power-supply id <i>number</i> temperature
Tree	temperature
Configurable	False
Platforms	Supported on all platforms

alarm-status *boolean*

Description	Indicates if the temperature of this component is currently in an alarm state
Context	platform power-supply id <i>number</i> temperature alarm-status <i>boolean</i>
Tree	alarm-status
Configurable	False
Platforms	Supported on all platforms

instant *number*

Description	The current temperature of this component
Context	platform power-supply id <i>number</i> temperature instant <i>number</i>
Tree	instant
Configurable	False
Platforms	Supported on all platforms

type *string*

Description	Power-supply type, as translated from the components EEPROM
Context	platform power-supply id <i>number</i> type <i>string</i>
Tree	type
Configurable	False
Platforms	Supported on all platforms

redundancy

Description	Top-level container for platform redundancy
Context	platform redundancy

Tree	redundancy
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

active-module *keyword*

Description	Control module currently active
Context	platform redundancy active-module <i>keyword</i>
Tree	active-module
Options	<ul style="list-style-type: none"> • A • B
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

failover-time *string*

Description	Date and time of the last control module failover
Context	platform redundancy failover-time <i>string</i>
Tree	failover-time
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

synchronization

Description	Top-level container for redundancy synchronization
Context	platform redundancy synchronization
Tree	synchronization
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

last-synchronization *string*

Description	Last date and time a synchronization of system files occurred
Context	platform redundancy synchronization last-synchronization <i>string</i>
Tree	last-synchronization

String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

overlay

Description	Top-level container for overlay synchronization
Context	platform redundancy synchronization overlay
Tree	overlay
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

last-synchronization *string*

Description	Last date and time a synchronization of the overlay occurred
Context	platform redundancy synchronization overlay last-synchronization string
Tree	last-synchronization
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

next-synchronization *string*

Description	Next date and time a synchronization of the overlay will occur
Context	platform redundancy synchronization overlay next-synchronization string
Tree	next-synchronization
String Length	20 to 32
Configurable	False
Platforms	7250 IXR-10, 7250 IXR-6

synchronization-frequency *number*

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.
--------------------	---

Context	platform redundancy synchronization overlay synchronization-frequency number
Tree	synchronization-frequency
Range	30 to 65535
Default	60
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

state keyword

Description	Current synchronization status
Context	platform redundancy synchronization state keyword
Tree	state
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
Platforms	7250 IXR-10, 7250 IXR-6

resource-management

Description	Container for managing resources in a system-wide context
Context	platform resource-management
Tree	resource-management
Configurable	True
Platforms	Supported on all platforms

tcam

Description	Container for managing the allocation of TCAM banks to different applications.
Context	platform resource-management tcam
Tree	tcam

Configurable	True
Platforms	Supported on all platforms

unified-forwarding-resources

Description	Container for managing Broadcom-specific UFT resources.
Context	platform resource-management unified-forwarding-resources
Tree	unified-forwarding-resources
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

allocated-extra-ip-host-entries *number*

Description	The extra number of host entries that have been allocated from UFT shared banks.
Context	platform resource-management unified-forwarding-resources allocated-extra-ip-host-entries <i>number</i>
Tree	allocated-extra-ip-host-entries
Range	0 to 262144
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

allocated-extra-mac-entries *number*

Description	The extra number of MAC address entries that have been allocated from UFT shared banks.
Context	platform resource-management unified-forwarding-resources allocated-extra-mac-entries <i>number</i>
Tree	allocated-extra-mac-entries
Range	0 to 262144
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

alpm *keyword*

Description	Controls the ALPM mode.
--------------------	-------------------------

If this is set to disabled then no UFT banks are allocated to ALPM.
 If this is set to enabled then 4 UFT shared banks are allocated to ALPM.
 If this is set to high-scale then 8 UFT shared banks are allocated to ALPM.
 This mode is not supported by 7220 IXR-D1.

Context	platform resource-management unified-forwarding-resources alpm <i>keyword</i>
Tree	alpm
Default	disabled
Options	<ul style="list-style-type: none"> • disabled • enabled • high-scale
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ipv6-128bit-lpm-entries *number*

Description	Sets the value for num_ipv6_lpm_128b_entries, which affects IP FIB scale. H2/H3 range: 0-1024 D1 range: 0-4096 D2/D3 range: 0-8192
Context	platform resource-management unified-forwarding-resources ipv6-128bit-lpm-entries <i>number</i>
Tree	ipv6-128bit-lpm-entries
Range	0 to 8192
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

requested-extra-ip-host-entries *number*

Description	<p>The extra number of host entries that are desired.</p> <p>The number of UFT shared banks that are reserved for IPv4 and IPv6 host entries is given by: $\min(N//X, P-A)$</p> <p>where: N = configured value of requested-extra-ip-host-entries X = the size of each shared bank, which is platform specific P-A = platform-specific number of shared banks, subtracting the ALPM banks</p> <p>requested-extra-ip-host-entries is interpreted in terms of IPv4 hosts (single-wide entries). IPv6 host entries are double-wide so 1 IPv4 host entry + 1 IPv6 host-entry counts as 3 entries.</p> <p>All UFT shared banks that are not reserved by ALPM and not reserved for extra IP host entries are used for extra MAC entries.</p>
--------------------	---

On D1 the default value is 48K entries, which provides 3 shared banks, max is 96K. On D2/D3 the default value is 128K entries, which provides 4 shared banks, max is 256K.

Context	platform resource-management unified-forwarding-resources requested-extra-ip-host-entries <i>number</i>
Tree	requested-extra-ip-host-entries
Range	0 to 262144
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

xdp-restart-required *boolean*

Description	Reads true if the user has committed a change to one or more of the configurable values in the uft container but has not yet restarted XDP so the operational values are still the values initialized at the last XDP restart.
Context	platform resource-management unified-forwarding-resources xdp-restart-required <i>boolean</i>
Tree	xdp-restart-required
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

resource-monitoring

Description	Enter the resource-monitoring context
Context	platform resource-monitoring
Tree	resource-monitoring
Configurable	True
Platforms	Supported on all platforms

acl

Description	Enter the acl context
Context	platform resource-monitoring acl
Tree	acl
Configurable	True
Platforms	Supported on all platforms

resource name *identityref*

Description	Enter the resource list instance
Context	platform resource-monitoring acl resource name <i>identityref</i>
Tree	resource
Configurable	True
Platforms	Supported on all platforms

name *identityref*

Description	The name of the ACL resource
Context	platform resource-monitoring acl resource name <i>identityref</i>
Options	<ul style="list-style-type: none"> • input-ipv4-filter-instances This 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-ipv4-filter-instances-routed This resource is used every time an IPv4 filter instance is created and applied to ingress traffic on routed subinterfaces. 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 routed subinterface using the IPv4 filter. • input-ipv4-filter-instances-bridged This resource is used every time an IPv4 filter instance is created and applied to ingress traffic on bridged subinterfaces. 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 bridged subinterface using the IPv4 filter. • input-ipv6-filter-instances This 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. • input-ipv6-filter-instances-routed This resource is used every time an IPv6 filter instance is created and applied to ingress traffic on routed subinterfaces. 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 routed subinterface using the IPv6 filter. • input-ipv6-filter-instances-bridged This resource is used every time an IPv6 filter instance is created and applied to ingress traffic on bridged subinterfaces. 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 bridged subinterface using the IPv6 filter.

- if-input-ipv4-stats
Resource pool of stats entries available for ingress IPv4 ACLs
- if-input-ipv6-stats
Resource pool of stats entries available for ingress IPv6 ACLs
- if-output-ipv4-stats
Resource pool of stats entries available for egress IPv4 ACLs
- if-output-ipv6-stats
Resource pool of stats entries available for egress IPv6 ACLs

Configurable	True
Platforms	Supported on all platforms

falling-threshold-log *number*

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
Context	platform resource-monitoring acl resource name <i>identityref</i> falling-threshold-log number
Tree	falling-threshold-log
Range	0 to 100
Default	70
Configurable	True
Platforms	Supported on all platforms

rising-threshold-log *number*

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
Context	platform resource-monitoring acl resource name <i>identityref</i> rising-threshold-log number
Tree	rising-threshold-log
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

datapath

Description	Container for monitoring datapath resources system-wide
Context	platform resource-monitoring datapath
Tree	datapath
Configurable	True
Platforms	Supported on all platforms

asic

Description	Container for monitoring datapath resources that are specific to a subset of the chipsets supported by SR Linux.
Context	platform resource-monitoring datapath asic
Tree	asic
Configurable	True
Platforms	Supported on all platforms

resource [name identityref](#)

Description	List of ASIC-specific datapath resources
Context	platform resource-monitoring datapath asic resource name identityref
Tree	resource
Configurable	True
Platforms	Supported on all platforms

name [identityref](#)

Description	The name of the ASIC-specific datapath resource.
Context	platform resource-monitoring datapath asic resource name identityref
Options	<ul style="list-style-type: none"> ip-lpm-ipv4-routes <p>Trident3: Reports the number of IPv4 entries in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of half-wide entries in all partitions (i.e. it assumes no IPv6 routes consume those entries). In ALPM mode, free entries is the Minimum Guaranteed Capacity returned by the BCM SDK.</p> <p>Trident3: Reports the number of IPv4 entries in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of half-wide entries in all partitions (i.e. it assumes no IPv6 routes consume those entries). In ALPM mode, free entries is the Minimum Guaranteed</p>

Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv4 routes installed in the FIB. Free entries is the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv4 entries in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of half-wide entries in all partitions (i.e. it assumes no IPv6 routes consume those entries). In ALPM mode, free entries is the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv4 routes installed in the FIB. Free entries is the Minimum Guaranteed Capacity returned by the BCM SDK. Monterey: Reports the number of IPv4 routes installed in the FIB. Free entries is the Minimum Guaranteed Capacity returned by the BCM SDK.

- ip-lpm-ipv6-shorter-routes

Trident3: Reports the number of IPv6 entries with prefix length less than 65 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of single-wide + double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length less than 65 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of single-wide + double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv6 entries with prefix length less than 65 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length less than 65 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of single-wide + double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Tomahawk3: Reports the number of IPv6 entries with prefix length less than 65 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Monterey: Reports the number of IPv6 entries with prefix length less than 65 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

- ip-lpm-ipv6-longer-routes

Trident3: Reports the number of IPv6 entries with prefix length greater than 64 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length greater than 64 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Tomahawk3: Reports the number of IPv6 entries with prefix length greater than 64 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Trident3: Reports the number of IPv6 entries with prefix length greater than 64 bits in the hardware LPM table. In non-ALPM mode, free entries is the remaining number of double-wide entries (i.e. it assumes no other types of routes consume those entries). In ALPM mode, free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

Tomahawk3: Reports the number of IPv6 entries with prefix length greater than 64 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK. Monterey: Reports the number of IPv6 entries with prefix length greater than 64 bits installed in the FIB. Free entries is based on the Minimum Guaranteed Capacity returned by the BCM SDK.

- exact-match-entries

Reports the number of half-wide entries used in the LEM table. Each MPLS ILM record uses one half-wide entry. Each IPv4 address used as a host route, ARP entry or subnet broadcast address requires a half-wide entry. An IPv6 address used as a host route, or ND entry requires a single-wide entry (2 half-wide entries). Free entries is the remaining number of half-wide entries.

- underlay-ecmp-groups

Underlay ECMP group resources.

Underlay ECMP group resources. ECMP groups are partitioned into overlay and underlay groups. The underlay partition is further subdivided into groups used for underlay ECMP and groups used for VP LAGs (EVPN M-H). This counts the utilization of the sub-resource used for ECMP.

- vp-lag-groups

VP LAG group resources.

VP LAG group resources. ECMP groups are partitioned into overlay and underlay groups. The underlay partition is further subdivided into groups used for underlay ECMP and groups used for VP LAGs (EVPN M-H). This counts the utilization of the sub-resource used for VP LAGs.

- overlay-ecmp-groups

Overlay ECMP group resources.

Overlay ECMP group resources. ECMP groups are partitioned into overlay and underlay groups. This counts the utilization of the overlay ECMP partition.

- underlay-ecmp-members

Underlay ECMP member resources.

Underlay ECMP member resources. ECMP members are partitioned into overlay and underlay. This counts the utilization of the partition used for underlay.

- overlay-ecmp-members

Overlay ECMP member resources.

Overlay ECMP member resources. ECMP members are partitioned into overlay and underlay. This counts the utilization of the partition used for overlay.

- underlay-egress-next-hops

Underlay egress next-hop resources.

Underlay egress next-hop resources. Egress next-hops are partitioned into overlay and underlay. This counts the utilization of the partition used for underlay.

- overlay-egress-next-hops

Overlay egress next-hop resources.

Overlay egress next-hop resources. Egress next-hops are partitioned into overlay and underlay. This counts the utilization of the partition used for overlay.

- dgpp-module-ids

DGPP module ID resources.

DGPP module ID resources. DGPPs are an aggregate id consisting of a module_id and a port_id. There are 64 modules and 120 ports per module. Each 'network' ARP entry (IP next-hop) needs a DGPP - the module_id is allocated against the network interface (port) and a port_id is allocated from within the module. A module_id will only be allocated when the first ArpEntry is added (freed when last is removed) but is owned exclusively by that network interface. A network interface may require more than one module_id - i.e. if there are 245 ArpEntries on ethernet-1/1 (possibly spread across multiple network-instance interfaces) then 3 module_ids are required.

- egress-vlan-translate-egress-vnis

EGR_VLAN_XLATE_1 resources.

EGR_VLAN_XLATE_1 resources. Corresponds to the 'EGR_VLAN_XLATE_1' HW table (8K entries). These entries are used for finding the egress VNI to be used for VXLAN packets.

- egress-vlan-translate-local-bias-pairs

EGR_VLAN_XLATE_2 resources.

EGR_VLAN_XLATE_2 resources. Corresponds to the 'EGR_VLAN_XLATE_2' HW table (24K entries). These entries are used for local bias (ES pruning).

- level-1-ecmp-groups

L1 ECMP group resources.

L1 ECMP group resources. ECMP FEC resources are divided into L1 ECMP FEC resources and L2 ECMP FEC resources. This counts the number of entries used in the L1 partition.

- level-2-ecmp-groups

L2 ECMP group resources.

L2 ECMP group resources. ECMP FEC resources are divided into L1 ECMP FEC resources and L2 ECMP FEC resources. This counts the number of entries used in the L2 partition.

- level-1-ecmp-members

L1 ECMP member resources.

L1 ECMP member resources. ECMP FEC member resources are divided into L1 and L2 resources. This counts the number of entries used in the L1 partition.

- level-2-ecmp-members

L2 ECMP member resources.

L2 ECMP member resources. ECMP FEC member resources are divided into L1 and L2 resources. This counts the number of entries used in the L2 partition.

- level-1-non-ecmp-fecs

L1 non-ECMP FEC resources.

L1 non-ECMP FEC resources. Non-ECMP FEC resources are divided into L1 and L2 resources. This counts the number of entries used in the L1 partition.

- level-2-non-ecmp-fecs

L2 non-ECMP FEC resources.

L2 non-ECMP FEC resources. Non-ECMP FEC resources are divided into L1 and L2 resources. This counts the number of entries used in the L2 partition.

Configurable	True
Platforms	Supported on all platforms

falling-threshold-log *number*

Description	Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the datapath resource in any linecard (if applicable) or forwarding complex or pipeline (if applicable) reaches this value in a falling direction
Context	platform resource-monitoring datapath asic resource name <i>identityref</i> falling-threshold-log <i>number</i>
Tree	falling-threshold-log
Range	0 to 100
Default	70
Configurable	True
Platforms	Supported on all platforms

rising-threshold-log *number*

Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the datapath resource in any linecard (if applicable) or forwarding complex or pipeline (if applicable) reaches this value in a rising direction
Context	platform resource-monitoring datapath asic resource name <i>identityref</i> rising-threshold-log <i>number</i>
Tree	rising-threshold-log
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

xdp

Description	Container for monitoring datapath resources that are generic in concept.
Context	platform resource-monitoring datapath xdp
Tree	xdp
Configurable	True
Platforms	Supported on all platforms

resource *name identityref*

Description	List of generic datapath resources
Context	platform resource-monitoring datapath xdp resource name <i>identityref</i>
Tree	resource
Configurable	True
Platforms	Supported on all platforms

name *identityref*

Description	The name of the XDP datapath resource. Some of these resources may be software only (i.e. no correspondence to a hardware table). Some of these resources may depend on multiple HW tables and when the utilization is reported it represents an aggregated or summarized view.
Context	platform resource-monitoring datapath xdp resource name <i>identityref</i>
Options	<ul style="list-style-type: none"> arp-nd-entries

IPv4 ARP and IPv6 neighbor discovery resources.

IPv4 ARP and IPv6 neighbor discovery resources. Each IPv4 ARP and each IPv6 neighbor entry counts as 1 used resource against a total that is platform dependent. This does not consider underlying ASIC resources.

- ip-hosts

IP host route resources.

IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks

IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks Tomahawk3: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries.

IP host route resources. Trident3: Reports the number of entries used in the IP host table. Every local host /32 route, ARP entry and IPv4 subnet broadcast address requires 1 entry. In non-ALPM operation every remote /32 route also requires 1 entry. Every local host /128 route, and ND entry requires 2 entries. In non-ALPM operation every remote /128 route also requires 2 entries. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks Tomahawk3: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries. Monterey: Reports the number of entries used in the IP host table. Every ARP entry and IPv4 subnet broadcast address requires 1 entry. Every ND entry requires 2 entries.

- ip-lpm-routes

IP longest prefix match route resources.

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes.

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes. Trident3 and Tomahawk3: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route (or index to IPv4 ALPM lookup) requires a half-wide entry. An IPv6 route (or index to IPv6 ALPM lookup) that is /64 or less requires a single-wide entry (2 half-

wide entries). An IPv6 route (or index to IPv6 ALPM lookup) that is more than /64 requires a double-wide entry (4 half-wide entries).

IP longest prefix match route resources. Jericho2: Reports the percentage utilization of the KAPS1 or KAPS2 table, whichever is higher. These tables are used for storing longest-prefix-match IPv4 and IPv6 routes. Trident3 and Tomahawk3: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route (or index to IPv4 ALPM lookup) requires a half-wide entry. An IPv6 route (or index to IPv6 ALPM lookup) that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route (or index to IPv6 ALPM lookup) that is more than /64 requires a double-wide entry (4 half-wide entries). Monterey: Reports the used and free number of half-wide entries in the hardware LPM table. An IPv4 route requires a half-wide entry. An IPv6 route that is /64 or less requires a single-wide entry (2 half-wide entries). An IPv6 route that is more than /64 requires a double-wide entry (4 half-wide entries).

- mac-addresses

MAC address resources.

MAC address resources. Reports the used number of entries, where 1 entry = 1 MAC address. Free entries reflects the total number of entries remaining in shared + dedicated UFT banks

- direct-next-hops

Direct next-hop resources.

Direct next-hop resources. Reports the number of entries, where 1 entry is used for every next-hop of an IP or MPLS route that is resolved directly to a local interface. This does not consider underlying ASIC resources.

- indirect-next-hops

Indirect next-hop resources.

Indirect next-hop resources. Reports the number of entries, where 1 entry is used for every next-hop of an IP route that is resolved by a non-local route. This does not consider underlying ASIC resources.

- tunnel-next-hops

Tunnel next-hop resources.

Tunnel next-hop resources. Reports the number of tunnel next-hop entries. For EVPN routes resolved by VXLAN, 1 entry is used for every <vni, vtep> pair. When a BGP IP route is resolved by an MPLS tunnel, 1 entry is used for every BGP next-hop of the route. This does not consider underlying ASIC resources.

- ecmp-groups

ECMP group resources.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups. Tomahawk3: Reports used number of ECMP groups.

ECMP group resources. Jericho2: Reports the used number of ECMP FECs, adding L1 ECMP FECs and L2 ECMP FECs. Trident3: Reports the used number of ECMP groups, adding overlay and underlay ECMP groups. Tomahawk3: Reports used number of ECMP groups. Monterey: Reports used number of ECMP groups.

- ecmp-members

ECMP member resources.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members. Tomahawk3: Reports used number of ECMP members.

ECMP member resources. Jericho2: Reports the used number of ECMP member FECs, adding L1 ECMP member FECs and L2 ECMP member FECs. Trident3: Reports the used number of ECMP members, adding overlay and underlay ECMP members. Tomahawk3: Reports used number of ECMP members. Monterey: Reports used number of ECMP members.

- egress-next-hops

Egress next-hop resources.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Tomahawk3: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

Egress next-hop resources. Trident3: Reports the number of entries used in the egress next-hop table, counting entries in the overlay partition and entries in the underlay partition. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Tomahawk3: Reports the number of entries used in the egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address. Monterey: Reports the number of entries used in the

egress next-hop table. 1 entry = 1 IPv4 next-hop address or 1 IPv6 next-hop address.

- lag-groups

LAG group resources.

LAG group resources. Reports the number of LAG resources used, including DGPP LAGs.

- lag-members

LAG member resources.

LAG member resources. Reports the number of LAG member resources used, including DGPP LAG members.

- subinterfaces

Subinterface resources.

Subinterface resources. There are a maximum of 127 subinterfaces per TH3 pipeline (limited by VFP/EFP TCAM resources). This counts the utilization of those resources.

- mpls-next-hops

One resource is used for every next-hop that pushes an MPLS label in every next-hop-group that is tied to an ILM entry that performs a 'swap'. One additional resource is used for every next-hop that pushes an MPLS label in every next-hop-group that is tied to an MPLS tunnel.

- mpls-incoming-labels

One resource is used for every MPLS ILM entry that performs either a 'swap' or a 'pop' operation.

- tunnels

Tunnel resources. One tunnel resource is used per VXLAN or MPLS tunnel endpoint.

Tunnel resources. One tunnel resource is used per VXLAN or MPLS tunnel endpoint. On TD3 systems this equates to a DVP resource.

Configurable

True

Platforms

Supported on all platforms

falling-threshold-log *number*

Description

Sets the threshold that triggers the generation of a NOTICE log whenever the utilization of the datapath resource in any linecard (if applicable) or forwarding complex or pipeline (if applicable) reaches this value in a falling direction

Context

[platform resource-monitoring datapath xdp resource name](#) *identityref* [falling-threshold-log number](#)

Tree

[falling-threshold-log](#)

Range

0 to 100

Default	70
Configurable	True
Platforms	Supported on all platforms

rising-threshold-log *number*

Description	Sets the threshold that triggers the generation of a WARNING log whenever the utilization of the datapath resource in any linecard (if applicable) or forwarding complex or pipeline (if applicable) reaches this value in a rising direction
Context	platform resource-monitoring datapath xdp resource name <i>identityref</i> rising-threshold-log <i>number</i>
Tree	rising-threshold-log
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

mtu

Description	Enter the mtu context
Context	platform resource-monitoring mtu
Tree	mtu
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

resource name *identityref*

Description	Enter the resource list instance
Context	platform resource-monitoring mtu resource name <i>identityref</i>
Tree	resource
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name *identityref*

Description	The name of the MTU resource
Context	platform resource-monitoring mtu resource name <i>identityref</i>

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. mpls-mtu MPLS MTU resource pool. One resource from this pool is consumed by every different MPLS MTU value used by the subinterfaces on the linecard forwarding-complex.
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

falling-threshold-log *number*

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.
Context	platform resource-monitoring mtu resource name <i>identityref</i> falling-threshold-log number
Tree	falling-threshold-log
Range	0 to 100
Default	70
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

rising-threshold-log *number*

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.
Context	platform resource-monitoring mtu resource name <i>identityref</i> rising-threshold-log number
Tree	rising-threshold-log
Range	0 to 100
Default	90

Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

qos

Description	Enter the qos context
Context	platform resource-monitoring qos
Tree	qos
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

resource [name identityref](#)

Description	Enter the resource list instance
Context	platform resource-monitoring qos resource name identityref
Tree	resource
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name [identityref](#)

Description	The name of the QoS resource
Context	platform resource-monitoring qos resource name identityref
Options	<ul style="list-style-type: none"> • classifier-profiles <p>A classifier-profile resource is used every time a different combination of IPv4 DSCP classifier and IPv6 DSCP classifier is applied to an ingress subinterface of the 7250 IXR IMM. There are 16 of these resources and one is always used by the combination of the default IPv4 DSCP classifier and the default IPv6 DSCP classifier.</p> • rewrite-profiles <p>On the 7250 IXR, a rewrite-profile resource is used every time a different combination of IPv4 DSCP rewrite-rule and IPv6 DSCP rewrite-rule is applied to an egress subinterface of the 7250 IXR IMM. There are 32 of these resources.</p> <p>On the 7250 IXR, a rewrite-profile resource is used every time a different combination of IPv4 DSCP rewrite-rule and IPv6 DSCP rewrite-rule is applied to an egress subinterface of the 7250 IXR IMM. There are 32 of these resources. On the SAS, a rewrite-profile is used every time a different combination of dot1p and MPLS traffic-class rewrite-rule is applied to an egress subinterface of the system. There are 15 of these resources.</p>

- `rewrite-policies`

A rewrite-policy resource is used every time a different DSCP or MPLS traffic-class rewrite-rule policy is applied to an egress subinterface of the 7250 IXR IMM. There are 32 of these resources.

Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

falling-threshold-log *number*

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
Context	platform resource-monitoring qos resource name <i>identityref</i> falling-threshold-log number
Tree	falling-threshold-log
Range	0 to 100
Default	70
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

rising-threshold-log *number*

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
Context	platform resource-monitoring qos resource name <i>identityref</i> rising-threshold-log number
Tree	rising-threshold-log
Range	0 to 100
Default	90
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

tcam

Description	Enter the tcam context
Context	platform resource-monitoring tcam
Tree	tcam
Configurable	True

Platforms Supported on all platforms

resource *name identityref*

Description Enter the resource list instance

Context [platform resource-monitoring tcam resource name identityref](#)

Tree [resource](#)

Configurable True

Platforms Supported on all platforms

name *identityref*

Description The name of the TCAM resource

Context [platform resource-monitoring tcam resource name identityref](#)

Options

- if-input-ipv4
Resource pool of TCAM entries used by IPv4 ACLs applied as subinterface-input filters
- if-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
- system-capture-ipv4
Resource pool of TCAM entries used by IPv4 capture-filter ACLs and IPv4 system-filter ACLs
- system-capture-ipv6
Resource pool of TCAM entries used by IPv6 capture-filter ACLs and IPv6 system-filter ACLs
- capture-ipv4

	Resource pool of TCAM entries used by IPv4 capture-filter ACLs
•	capture-ipv6
	Resource pool of TCAM entries used by IPv6 capture-filter ACLs
•	if-output-cpm-ipv4
	Resource pool of TCAM entries used by IPv4 egress ACLs and cpm-filter ACLs
•	if-output-cpm-ipv6
	Resource pool of TCAM entries used by IPv6 egress ACLs and cpm-filter ACLs
•	if-input-mac
	Resource pool of TCAM entries used by MAC ACLs applied as subinterface-input filters
•	if-output-cpm-mac
	Resource pool of TCAM entries used by MAC egress ACLs and MAC cpm-filter ACLs
•	policy-forwarding-ipv4
	Resource pool of TCAM entries used by IPv4 policy-forwarding entries
Configurable	True
Platforms	Supported on all platforms

falling-threshold-log *number*

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. On platforms that support dynamic TCAM the utilization considers free-dynamic, and not free-static.
Context	platform resource-monitoring tcam resource name <i>identityref</i> falling-threshold-log <i>number</i>
Tree	falling-threshold-log
Range	0 to 100
Default	70
Configurable	True
Platforms	Supported on all platforms

rising-threshold-log *number*

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 On platforms that support dynamic TCAM the utilization considers free-dynamic, and not free-static.
Context	platform resource-monitoring tcam resource name <i>identityref</i> rising-threshold-log <i>number</i>
Tree	rising-threshold-log
Range	0 to 100
Default	90
Configurable	True
Platforms	Supported on all platforms

8 qos

```

qos
+ classifiers
+ dot1p-policy name string
+ dot1p value number
+ drop-probability keyword
+ forwarding-class keyword
+ dscp-policy name string
+ dscp value number
+ drop-probability keyword
+ forwarding-class keyword
+ mpls-traffic-class-policy name string
+ traffic-class value number
+ drop-probability keyword
+ forwarding-class keyword
+ vxlan-default reference
+ explicit-congestion-notification
+ ecn-dscp-policy reference
+ policer-templates
+ policer-template name string
+ policer index number
+ committed-burst-size number
+ committed-rate-kbps number
+ exceed-action
+ drop-probability keyword
+ forwarding-class fc keyword
+ forwarding-type keyword
+ maximum-burst-size number
+ peak-rate-kbps number
+ violate-action
+ drop
+ drop-probability keyword
+ statistics-mode keyword
+ queue-templates
+ queue-template name string
+ active-queue-management
+ ecn-slope ecn-drop-probability keyword
+ max-probability number
+ max-threshold-percent number
+ min-threshold-percent number
+ weight-factor number
+ wred-slope traffic-type keyword drop-probability keyword
+ max-probability number
+ max-threshold-percent number
+ min-threshold-percent number
+ queue-depth
+ high-threshold-bytes number
+ maximum-burst-size number
+ rewrite-rules
+ dot1p-policy name string
+ map forwarding-class keyword
+ dot1p number
+ drop-probability drop-probability keyword
+ dot1p number
+ dscp-policy name string
+ map forwarding-class keyword
+ drop-probability drop-probability keyword
+ dscp (number | keyword)
+ dscp (number | keyword)

```

```
+ mpls-traffic-class-policy name string
+ map forwarding-class keyword
+ drop-probability drop-probability keyword
+ traffic-class number
+ traffic-class number
```

8.1 qos Descriptions

qos

Description	Top-level container for QoS data
Context	qos
Tree	qos
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

classifiers

Description	Enter the classifiers context
Context	qos classifiers
Tree	classifiers
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dot1p-policy [name string](#)

Description	Enter the dot1p-policy list instance
Context	qos classifiers dot1p-policy name string
Tree	dot1p-policy
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

name *string*

Description	User-configured name for a 802.1p priority code point classification policy The name 'default' is reserved for the system default DSCP classifier.
Context	qos classifiers dot1p-policy name string
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dot1p value number

Description	Enter the dot1p list instance
Context	qos classifiers dot1p-policy name <i>string</i> dot1p value number
Tree	dot1p
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

value number

Description	Enter the value context
Context	qos classifiers dot1p-policy name <i>string</i> dot1p value number
Range	0 to 7
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

drop-probability keyword

Description	The drop probability to which the dot1p value is mapped
Context	qos classifiers dot1p-policy name <i>string</i> dot1p value number drop-probability keyword
Tree	drop-probability
Options	<ul style="list-style-type: none"> • low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. • medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. • high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

forwarding-class keyword

Description	The forwarding class to which the dot1p value is mapped
Context	qos classifiers dot1p-policy name <i>string</i> dot1p value number forwarding-class keyword

Tree	forwarding-class
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dscp-policy *name string*

Description	Enter the dscp-policy list instance
Context	qos classifiers dscp-policy name string
Tree	dscp-policy
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

name *string*

Description	User-configured name for a DSCP classification policy The name 'default' is reserved for the system default DSCP classifier.
Context	qos classifiers dscp-policy name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dscp *value number*

Description	Enter the dscp list instance
Context	qos classifiers dscp-policy name string dscp value number
Tree	dscp
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

value number

Description	Enter the value context
Context	qos classifiers dscp-policy name <i>string</i> dscp value number
Range	0 to 63
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability keyword

Description	The drop probability to which the DSCP value is mapped
Context	qos classifiers dscp-policy name <i>string</i> dscp value number drop-probability keyword
Tree	drop-probability
Options	<ul style="list-style-type: none"> • low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. • medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. • high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

forwarding-class keyword

Description	The forwarding class to which the DSCP value is mapped
Context	qos classifiers dscp-policy name <i>string</i> dscp value number forwarding-class keyword
Tree	forwarding-class
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5

	<ul style="list-style-type: none"> • fc6 • fc7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

mpls-traffic-class-policy *name string*

Description	Enter the mpls-traffic-class-policy list instance
Context	qos classifiers mpls-traffic-class-policy name string
Tree	mpls-traffic-class-policy
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name *string*

Description	User-configured name for an MPLS traffic-class classification policy The name 'default' is reserved for the system default MPLS TC classifier.
Context	qos classifiers mpls-traffic-class-policy name string
String Length	1 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

traffic-class *value number*

Description	Enter the traffic-class list instance
Context	qos classifiers mpls-traffic-class-policy name string traffic-class value number
Tree	traffic-class
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

value *number*

Description	A single traffic-class value
Context	qos classifiers mpls-traffic-class-policy name string traffic-class value number
Range	0 to 7

Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

drop-probability *keyword*

Description	The drop probability to which the traffic-class value is mapped
Context	qos classifiers mpls-traffic-class-policy name <i>string</i> traffic-class value <i>number</i> drop-probability keyword
Tree	drop-probability
Options	<ul style="list-style-type: none"> • low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. • medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. • high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

forwarding-class *keyword*

Description	The forwarding class to which the traffic-class value is mapped
Context	qos classifiers mpls-traffic-class-policy name <i>string</i> traffic-class value <i>number</i> forwarding-class keyword
Tree	forwarding-class
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

vxlan-default *reference*

Description	Reference to the name of a DSCP classifier policy that applies to terminating VXLAN packets.
Context	qos classifiers vxlan-default <i>reference</i>
Tree	vxlan-default
Reference	qos classifiers dscp-policy name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

explicit-congestion-notification

Description	Enable the explicit-congestion-notification context
Context	qos explicit-congestion-notification
Tree	explicit-congestion-notification
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

ecn-dscp-policy *reference*

Description	Reference to the DSCP rewrite policy to use when DSCP rewrite is required as a side effect of ECN remarking. This is required configuration in order to globally enable ECN on J2 platforms.
Context	qos explicit-congestion-notification ecn-dscp-policy <i>reference</i>
Tree	ecn-dscp-policy
Reference	qos rewrite-rules dscp-policy name <i>string</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

policer-templates

Description	Policer templates used for subinterface traffic metering.
Context	qos policer-templates
Tree	policer-templates
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

policer-template *name string*

Description	List of policer templates.
Context	qos policer-templates policer-template name string
Tree	policer-template
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

name *string*

Description	The name assigned to the policer template.
Context	qos policer-templates policer-template name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

policer *index number*

Description	The list of policer instances belonging to the template definition.
Context	qos policer-templates policer-template name string policer index number
Tree	policer
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

index *number*

Description	The policer index
Context	qos policer-templates policer-template name string policer index number
Range	1 to 32
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

committed-burst-size *number*

Description	Maximum CIR bucket depth in bytes.
Context	qos policer-templates policer-template name string policer index number committed-burst-size number

Tree	committed-burst-size
Units	bytes
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

committed-rate-kbps *number*

Description	The committed information rate (CIR) of the policer, defined in kilobits (1024 bits) per second.
Context	qos policer-templates policer-template name <i>string</i> policer index <i>number</i> committed-rate-kbps <i>number</i>
Tree	committed-rate-kbps
Units	kbps
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

exceed-action

Description	Container with options that specify the handling of packets that the policer has determined are exceeding (yellow)
Context	qos policer-templates policer-template name <i>string</i> policer index <i>number</i> exceed-action
Tree	exceed-action
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability *keyword*

Description	Recolor exceeding packets to the specified drop-probability level
Context	qos policer-templates policer-template name <i>string</i> policer index <i>number</i> exceed-action drop-probability <i>keyword</i>
Tree	drop-probability
Default	medium
Options	<ul style="list-style-type: none"> low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow.

- high
Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.

Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

forwarding-class *fc keyword*

Description	Enter the forwarding-class list instance
Context	qos policer-templates policer-template name string policer index number forwarding-class fc keyword
Tree	forwarding-class
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

fc *keyword*

Description	A forwarding class that has traffic to match to the policer.
Context	qos policer-templates policer-template name string policer index number forwarding-class fc keyword
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

forwarding-type *keyword*

Description	The list of forwarding types, belonging to this forwarding-class, to match to the policer. If none are specified, this implies ALL forwarding types.
Context	qos policer-templates policer-template name string policer index number forwarding-class fc keyword forwarding-type keyword
Tree	forwarding-type

Options	<ul style="list-style-type: none"> unicast A packet is 'unicast' if the destination address is unicast and it matches an entry in the FIB unknown-unicast A packet is 'unknown-unicast' if the destination address is unicast but it doesn't match any entry in the FIB and is therefore conventionally flooded broadcast A packet is 'broadcast' if the destination address is a broadcast address. multicast A packet is 'multicast' if the destination address is a multicast address.
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1
Max. Elements	4

maximum-burst-size *number*

Description	Maximum PIR bucket depth in bytes.
Context	qos policer-templates policer-template name <i>string</i> policer index number <i>number</i> maximum-burst-size number
Tree	maximum-burst-size
Units	bytes
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

peak-rate-kbps *number*

Description	The peak information rate (PIR) of the policer, defined in kilobits (1024 bits) per second.
Context	qos policer-templates policer-template name <i>string</i> policer index number <i>number</i> peak-rate-kbps number
Tree	peak-rate-kbps
Units	kbps
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

violate-action

Description	Container with options that specify the handling of packets that the policer has determined are violating (red)
Context	qos policer-templates policer-template name <i>string</i> policer index <i>number</i> violate-action
Tree	violate-action
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop

Description	Violating packets should be dropped immediately
Context	qos policer-templates policer-template name <i>string</i> policer index <i>number</i> violate-action drop
Tree	drop
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability *keyword*

Description	Recolor violating packets to the specified drop-probability level
Context	qos policer-templates policer-template name <i>string</i> policer index <i>number</i> violate-action drop-probability <i>keyword</i>
Tree	drop-probability
Default	high
Options	<ul style="list-style-type: none"> • low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. • medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. • high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

statistics-mode *keyword*

Description	The statistics mode of all policers belonging to this template
Context	qos policer-templates policer-template name <i>string</i> statistics-mode <i>keyword</i>
Tree	statistics-mode
Default	violating-focus
Options	<ul style="list-style-type: none"> violating-focus In this statistics mode only 4 counters are provided: accepted-packets, accepted-octets, violating-packets, violating-octets forwarding-focus In this statistics mode only 4 counters are provided: committed-packets, committed-octets, exceeding-packets, exceeding-octets
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

queue-templates

Description	Enter the queue-templates context
Context	qos queue-templates
Tree	queue-templates
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

queue-template *name string*

Description	List of queue templates that can be applied to egress queues or VOQ sets The 7250 IXR-6/10 platforms supports a maximum 8 queue-templates. The 7220-D2/D3/H2/H3 platforms support a maximum of 64 queue-templates.
Context	qos queue-templates queue-template name <i>string</i>
Tree	queue-template
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1
Max. Elements	64

name *string*

Description	The name of the queue template
--------------------	--------------------------------

The queue template with the special name 'default' is used when a queue-template reference is missing.

Context	qos queue-templates queue-template name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

active-queue-management

Description	Enable the active-queue-management context
Context	qos queue-templates queue-template name <i>string</i> active-queue-management
Tree	active-queue-management
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

ecn-slope [ecn-drop-probability](#) *keyword*

Description	List of ECN slopes.
Context	qos queue-templates queue-template name <i>string</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i>
Tree	ecn-slope
Configurable	True
Platforms	Supported on all platforms

ecn-drop-probability *keyword*

Description	The drop probability to which the ECN slope applies.
Context	qos queue-templates queue-template name <i>string</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i>
Options	<ul style="list-style-type: none"> low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.

	<ul style="list-style-type: none"> all <p>All traffic, consisting of traffic marked low, medium and high drop-probability.</p>
Configurable	True
Platforms	Supported on all platforms

max-probability *number*

Description	<p>The maximum probability of marking a packet (at or above the max-threshold).</p> <p>On TD3/TH3 max-probability has a limited set of discrete values: 1,2,3,4,5,6,7,8,9,10,25,50,75,100. The user is allowed to enter any value but the system will choose the next-highest value that is supported.</p> <p>A slope is disabled by setting min-threshold-percent=100, max-threshold-percent=100 and max-probability=0.</p>
Context	qos queue-templates queue-template name <i>string</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i> max-probability <i>number</i>
Tree	max-probability
Range	0 to 100
Default	0
Configurable	True
Platforms	Supported on all platforms

max-threshold-percent *number*

Description	<p>The percentage of the MBS that corresponds to the ECN maximum threshold parameter.</p> <p>A slope is disabled by setting min-threshold-percent=100, max-threshold-percent=100 and max-probability=0.</p>
Context	qos queue-templates queue-template name <i>string</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i> max-threshold-percent <i>number</i>
Tree	max-threshold-percent
Range	0 to 100
Default	100
Configurable	True
Platforms	Supported on all platforms

min-threshold-percent *number*

Description	The percentage of the MBS that corresponds to the ECN minimum threshold parameter. A slope is disabled by setting min-threshold-percent=100, max-threshold-percent=100 and max-probability=0.
Context	qos queue-templates queue-template name <i>string</i> active-queue-management ecn-slope ecn-drop-probability <i>keyword</i> min-threshold-percent <i>number</i>
Tree	min-threshold-percent
Range	0 to 100
Default	100
Configurable	True
Platforms	Supported on all platforms

weight-factor *number*

Description	Weight factor to use in the calculation of the current (average weighted) queue depth.
Context	qos queue-templates queue-template name <i>string</i> active-queue-management weight-factor <i>number</i>
Tree	weight-factor
Range	0 to 15
Default	0
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

wred-slope [traffic-type](#) *keyword* [drop-probability](#) *keyword*

Description	List of WRED slopes.
Context	qos queue-templates queue-template name <i>string</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i>
Tree	wred-slope
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

traffic-type *keyword*

Description	The traffic type to which the WRED slope applies.
--------------------	---

Context	qos queue-templates queue-template name <i>string</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i>
Options	<ul style="list-style-type: none"> • tcp Refers to IPv4/IPv6 packets with a protocol/next-header indicating a value of 6. • non-tcp Refers to all packets that are not IPv4/IPv6 packets with a protocol/next-header indicating a value of 6. • all Refers to all traffic, whether it is TCP or non-TCP.
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability *keyword*

Description	The drop probability to which the WRED slope applies.
Context	qos queue-templates queue-template name <i>string</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i>
Options	<ul style="list-style-type: none"> • low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. • medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. • high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

max-probability *number*

Description	<p>The maximum probability of dropping a packet (at or above the max-threshold).</p> <p>A slope is disabled by setting min-threshold-percent=100, max-threshold-percent=100 and max-probability=0</p>
Context	qos queue-templates queue-template name <i>string</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> max-probability <i>number</i>

Tree	max-probability
Range	0 to 100
Default	0
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

max-threshold-percent *number*

Description	The percentage of the MBS that corresponds to the WRED maximum threshold parameter. A slope is disabled by setting min-threshold-percent=100, max-threshold-percent=100 and max-probability=0
Context	qos queue-templates queue-template name <i>string</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> max-threshold-percent <i>number</i>
Tree	max-threshold-percent
Range	0 to 100
Default	100
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

min-threshold-percent *number*

Description	The percentage of the MBS that corresponds to the WRED minimum threshold parameter. A slope is disabled by setting min-threshold-percent=100, max-threshold-percent=100 and max-probability=0
Context	qos queue-templates queue-template name <i>string</i> active-queue-management wred-slope traffic-type <i>keyword</i> drop-probability <i>keyword</i> min-threshold-percent <i>number</i>
Tree	min-threshold-percent
Range	0 to 100
Default	100
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

queue-depth

Description	Enter the queue-depth context
Context	qos queue-templates queue-template name <i>string</i> queue-depth
Tree	queue-depth
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

high-threshold-bytes *number*

Description	<p>The queue depth that, when crossed in a rising direction, triggers a hardware interrupt and a recording of the current system time.</p> <p>The default value of 0 disables the functionality.</p> <p>On J2 systems this parameter applies to a set of VOQs (and therefore to unicast traffic only). On TD3/TH3 systems this parameter applies to a unicast queue only; the configuration of this leaf is ignored when the queue-template is attached to a multicast-queue.</p> <p>On TD3 the threshold is rounded up the nearest multiple of 2048 bytes. On J2 the threshold is rounded up to the nearest multiple of 4096 bytes. On TH3 the threshold is rounded up to the nearest multiple of 254 bytes.</p>
Context	qos queue-templates queue-template name <i>string</i> queue-depth high-threshold-bytes <i>number</i>
Tree	high-threshold-bytes
Default	0
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

maximum-burst-size *number*

Description	<p>Maximum queue depth in bytes. MBS buffer space is not guaranteed.</p> <p>On J2 systems this parameter applies to a set of VOQs and the default is 256 MB (268435456 bytes).</p> <p>On TD3, TH3 and SAS systems this parameter applies to an egress queue and the default value of zero instructs the forwarding chip to apply its own limit based on 'alpha'. A non-zero value disables 'alpha'.</p> <p>On SAS systems the actual hardware value is a multiple of 2048 bytes.</p> <p>Must be non-zero/non-default in order to add the active-queue-management presence container.</p>
Context	qos queue-templates queue-template name <i>string</i> queue-depth maximum-burst-size <i>number</i>

Tree	maximum-burst-size
Default	0
Units	bytes
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

rewrite-rules

Description	Enter the rewrite-rules context
Context	qos rewrite-rules
Tree	rewrite-rules
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dot1p-policy [name string](#)

Description	Enter the dot1p-policy list instance
Context	qos rewrite-rules dot1p-policy name string
Tree	dot1p-policy
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

name *string*

Description	User-configured name for an 802.1p priority code point rewrite policy.
Context	qos rewrite-rules dot1p-policy name string
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

map [forwarding-class keyword](#)

Description	Enter the map list instance
Context	qos rewrite-rules dot1p-policy name string map forwarding-class keyword
Tree	map
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

forwarding-class *keyword*

Description The forwarding-class value

Context [qos rewrite-rules dot1p-policy name string map forwarding-class keyword](#)

Options

- fc0
- fc1
- fc2
- fc3
- fc4
- fc5
- fc6
- fc7

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dot1p *number*

Description The dot1p marking to be used for all packets associated with the FC, except those with a drop-probability-specific override.

Context [qos rewrite-rules dot1p-policy name string map forwarding-class keyword dot1p number](#)

Tree [dot1p](#)

Range 0 to 7

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

drop-probability [drop-probability keyword](#)

Description Enter the drop-probability list instance

Context [qos rewrite-rules dot1p-policy name string map forwarding-class keyword drop-probability drop-probability keyword](#)

Tree [drop-probability](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

drop-probability *keyword*

Description	A drop probability level within the FC for which a different remarking is desired.
Context	qos rewrite-rules dot1p-policy name string map forwarding-class keyword drop-probability drop-probability keyword
Options	<ul style="list-style-type: none"> low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dot1p *number*

Description	The dot1p marking to be used for this specific drop-probability
Context	qos rewrite-rules dot1p-policy name string map forwarding-class keyword drop-probability drop-probability keyword dot1p number
Tree	dot1p
Range	0 to 7
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dscp-policy *name string*

Description	Enter the dscp-policy list instance
Context	qos rewrite-rules dscp-policy name string
Tree	dscp-policy
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

name *string*

Description	User-configured name for a DSCP rewrite policy.
--------------------	---

Context	qos rewrite-rules dscp-policy name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

map forwarding-class *keyword*

Description	Enter the map list instance
Context	qos rewrite-rules dscp-policy name <i>string</i> map forwarding-class <i>keyword</i>
Tree	map
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

forwarding-class *keyword*

Description	The forwarding-class value
Context	qos rewrite-rules dscp-policy name <i>string</i> map forwarding-class <i>keyword</i>
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability [drop-probability](#) *keyword*

Description	Enter the drop-probability list instance
Context	qos rewrite-rules dscp-policy name <i>string</i> map forwarding-class <i>keyword</i> drop-probability drop-probability <i>keyword</i>
Tree	drop-probability
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

drop-probability *keyword*

Description	A drop probability level within the FC for which a different remarking is desired.
Context	<code>qos rewrite-rules dscp-policy name string map forwarding-class keyword drop-probability drop-probability keyword</code>
Options	<ul style="list-style-type: none"> low Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green. medium Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow. high Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dscp (*number* | *keyword*)

Description	The DSCP marking to be used for this specific drop-probability
Context	<code>qos rewrite-rules dscp-policy name string map forwarding-class keyword drop-probability drop-probability keyword dscp (number keyword)</code>
Tree	<code>dscp</code>
Range	0 to 63
Options	<ul style="list-style-type: none"> CS0 LE CS1 AF11 AF12 AF13 CS2 AF21 AF22 AF23 CS3 AF31 AF32

	<ul style="list-style-type: none"> • AF33 • CS4 • AF41 • AF42 • AF43 • CS5 • EF • CS6 • CS7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

dscp (*number | keyword*)

Description	The DSCP marking to be used for all packets associated with the FC, except those with a drop-probability-specific override.
Context	qos rewrite-rules dscp-policy name <i>string</i> map forwarding-class keyword dscp (number keyword)
Tree	dscp
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

	<ul style="list-style-type: none"> • AF43 • CS5 • EF • CS6 • CS7
Configurable	True
Platforms	Supported on all platforms except 7220 IXR-D1

mpls-traffic-class-policy *name string*

Description	Enter the mpls-traffic-class-policy list instance
Context	qos rewrite-rules mpls-traffic-class-policy name string
Tree	mpls-traffic-class-policy
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name *string*

Description	User-configured name for an MPLS traffic-class rewrite policy.
Context	qos rewrite-rules mpls-traffic-class-policy name string
String Length	1 to 255
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

map forwarding-class *keyword*

Description	Enter the map list instance
Context	qos rewrite-rules mpls-traffic-class-policy name string map forwarding-class keyword
Tree	map
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

forwarding-class *keyword*

Description	The forwarding-class value
--------------------	----------------------------

Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i> map forwarding-class <i>keyword</i>
Options	<ul style="list-style-type: none"> • fc0 • fc1 • fc2 • fc3 • fc4 • fc5 • fc6 • fc7
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

drop-probability [drop-probability](#) *keyword*

Description	Enter the drop-probability list instance
Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i> map forwarding-class <i>keyword</i> drop-probability drop-probability <i>keyword</i>
Tree	drop-probability
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

drop-probability *keyword*

Description	A drop probability level within the FC for which a different remarking is desired.
Context	qos rewrite-rules mpls-traffic-class-policy name <i>string</i> map forwarding-class <i>keyword</i> drop-probability drop-probability <i>keyword</i>
Options	<ul style="list-style-type: none"> • low <p>Traffic that should be dropped last when there is congestion. Internally this is traffic that is colored green.</p> • medium <p>Traffic that should be dropped before green traffic but after red traffic when there is congestion. Internally this is traffic that is colored yellow.</p> • high <p>Traffic that should be dropped first when there is congestion. Internally this is traffic that is colored red.</p>
Configurable	True

Platforms 7250 IXR-10, 7250 IXR-6

traffic-class *number*

Description The MPLS traffic class marking to be used for this specific drop-probability

Context [qos rewrite-rules mpls-traffic-class-policy name](#) *string* [map forwarding-class](#) *keyword* [drop-probability drop-probability](#) *keyword* [traffic-class](#) *number*

Tree [traffic-class](#)

Range 0 to 7

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

traffic-class *number*

Description The MPLS traffic class marking to be used for all packets associated with the FC, except those with a drop-probability-specific override.

Context [qos rewrite-rules mpls-traffic-class-policy name](#) *string* [map forwarding-class](#) *keyword* [traffic-class](#) *number*

Tree [traffic-class](#)

Range 0 to 7

Configurable True

Platforms 7250 IXR-10, 7250 IXR-6

9 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
+ remove boolean
+ replace number
+ communities
+ add reference
+ remove reference
+ replace reference
+ local-preference
+ set number
+ origin
+ set keyword
+ reject
+ statement sequence-id number
+ action
+ accept
+ bgp
+ as-path
+ prepend
+ as-number (number | keyword)
+ repeat-n number
+ remove boolean
+ replace number
+ communities
+ add reference
+ remove reference
+ replace reference
+ local-preference
+ set number
+ origin
+ set keyword
+ reject
+ match
+ bgp
+ as-path-length
+ operator keyword
+ unique boolean
+ value number
+ as-path-set reference
+ community-set reference
+ evpn
+ route-type number
+ family identityref
+ isis
+ level number
+ route-type keyword

```

```
+ ospf
  + area-id
  + instance-id number
  + route-type identityref
  + prefix-set reference
  + protocol identityref
+ prefix-set name string
  + prefix ip-prefix (ipv4-prefix | ipv6-prefix) mask-length-range string
```

9.1 routing-policy Descriptions

routing-policy

Description	Top-level container for all routing policy configuration
Context	routing-policy
Tree	routing-policy
Configurable	True
Platforms	Supported on all platforms

as-path-set *name string*

Description	AS Path regular expressions for use in policy entries
Context	routing-policy as-path-set name string
Tree	as-path-set
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	A name used to identify the AS path regular expression
Context	routing-policy as-path-set name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

expression *string*

Description	A regular expression where each AS number is an elemental term
Context	routing-policy as-path-set name string expression string
Tree	expression
String Length	1 to 65535
Configurable	True
Platforms	Supported on all platforms

community-set *name string*

Description	List of BGP community sets containing standard and large BGP communities
Context	routing-policy community-set name string
Tree	community-set
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	A name used to identify the community set
Context	routing-policy community-set name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

member (*bgp-std-community-type | bgp-std-community-regexp-type | identityref | bgp-large-community-type | bgp-large-community-regexp-type*)

Description	A standard BGP community value, regular expression or well-known name or else a large BGP community value or regular expression
Context	routing-policy community-set name string member (<i>bgp-std-community-type bgp-std-community-regexp-type identityref bgp-large-community-type bgp-large-community-regexp-type</i>)
Tree	member
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
Platforms	Supported on all platforms
Min. Elements	1

policy name *string*

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.
Context	routing-policy policy name <i>string</i>
Tree	policy
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	A name used to identify the policy
Context	routing-policy policy name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

default-action

Description	Actions for routes that do not match any policy entry
Context	routing-policy policy name <i>string</i> default-action
Tree	default-action
Configurable	True
Platforms	Supported on all platforms

accept

Description	Accept action
Context	routing-policy policy name <i>string</i> default-action accept
Tree	accept
Configurable	True
Platforms	Supported on all platforms

bgp

Description	Enable the bgp context
--------------------	------------------------

Context	routing-policy policy name <i>string</i> default-action accept bgp
Tree	bgp
Configurable	True
Platforms	Supported on all platforms

as-path

Description	Modify AS Path attribute of routes
Context	routing-policy policy name <i>string</i> default-action accept bgp as-path
Tree	as-path
Configurable	True
Platforms	Supported on all platforms

prepend

Description	Prepend a BGP AS number to the AS Path attribute of routes
Context	routing-policy policy name <i>string</i> default-action accept bgp as-path prepend
Tree	prepend
Configurable	True
Platforms	Supported on all platforms

as-number (*number* | *keyword*)

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.
Context	routing-policy policy name <i>string</i> default-action accept bgp as-path prepend as-number (<i>number</i> <i>keyword</i>)
Tree	as-number
Range	1 to 4294967295
Options	<ul style="list-style-type: none"> • auto
Configurable	True
Platforms	Supported on all platforms

repeat-n *number*

Description	The number of repetitions of the prepended AS number
Context	routing-policy policy name string default-action accept bgp as-path prepend repeat-n <i>number</i>
Tree	repeat-n
Range	1 to 50
Default	1
Configurable	True
Platforms	Supported on all platforms

remove *boolean*

Description	Clear the AS path to make it empty.
Context	routing-policy policy name string default-action accept bgp as-path remove <i>boolean</i>
Tree	remove
Configurable	True
Platforms	Supported on all platforms

replace *number*

Description	Clear the existing AS path and replace it a new AS_SEQUENCE containing the listed AS numbers.
Context	routing-policy policy name string default-action accept bgp as-path replace <i>number</i>
Tree	replace
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

communities

Description	Modify BGP communities attached to routes
Context	routing-policy policy name string default-action accept bgp communities
Tree	communities
Configurable	True
Platforms	Supported on all platforms

add reference

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.
Context	routing-policy policy name string default-action accept bgp communities add reference
Tree	add
Reference	routing-policy community-set name string
Configurable	True
Platforms	Supported on all platforms

remove reference

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.
Context	routing-policy policy name string default-action accept bgp communities remove reference
Tree	remove
Reference	routing-policy community-set name string
Configurable	True
Platforms	Supported on all platforms

replace reference

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.
Context	routing-policy policy name string default-action accept bgp communities replace reference
Tree	replace
Reference	routing-policy community-set name string
Configurable	True
Platforms	Supported on all platforms

local-preference

Description	Enter the local-preference context
Context	routing-policy policy name <i>string</i> default-action accept bgp local-preference
Tree	local-preference
Configurable	True
Platforms	Supported on all platforms

set number

Description	The new value of LOCAL_PREF to write into the matching BGP routes
Context	routing-policy policy name <i>string</i> default-action accept bgp local-preference set number
Tree	set
Configurable	True
Platforms	Supported on all platforms

origin

Description	Enter the origin context
Context	routing-policy policy name <i>string</i> default-action accept bgp origin
Tree	origin
Configurable	True
Platforms	Supported on all platforms

set keyword

Description	The new value of the ORIGIN attribute to write into the matching BGP routes
Context	routing-policy policy name <i>string</i> default-action accept bgp origin set keyword
Tree	set
Options	<ul style="list-style-type: none"> • igp • egp • incomplete
Configurable	True
Platforms	Supported on all platforms

reject

Description	Reject action
Context	routing-policy policy name <i>string</i> default-action reject
Tree	reject
Configurable	True
Platforms	Supported on all platforms

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

Description	Policy statements group conditions and actions within a policy definition. They are evaluated in the order of their sequence id.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i>
Tree	statement
Configurable	True
Platforms	Supported on all platforms

sequence-id *number*

Description	Number indicating when this policy statement should be evaluated relative to other policy statements Lower numbered statements are evaluated before higher numbered statements.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i>
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

action

Description	Policy actions
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action
Tree	action
Configurable	True
Platforms	Supported on all platforms

accept

Description	Accept action
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept
Tree	accept
Configurable	True
Platforms	Supported on all platforms

bgp

Description	Enable the bgp context
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp
Tree	bgp
Configurable	True
Platforms	Supported on all platforms

as-path

Description	Modify AS Path attribute of routes
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path
Tree	as-path
Configurable	True
Platforms	Supported on all platforms

prepend

Description	Prepend a BGP AS number to the AS Path attribute of routes
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path prepend
Tree	prepend
Configurable	True
Platforms	Supported on all platforms

as-number (*number* | *keyword*)

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.

Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path prepend as-number (<i>number</i> <i>keyword</i>)
Tree	as-number
Range	1 to 4294967295
Options	<ul style="list-style-type: none"> • auto
Configurable	True
Platforms	Supported on all platforms

repeat-n *number*

Description	The number of repetitions of the prepended AS 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
Range	1 to 50
Default	1
Configurable	True
Platforms	Supported on all platforms

remove *boolean*

Description	Clear the AS path to make it empty.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path remove <i>boolean</i>
Tree	remove
Configurable	True
Platforms	Supported on all platforms

replace *number*

Description	Clear the existing AS path and replace it a new AS_SEQUENCE containing the listed AS numbers.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp as-path replace <i>number</i>
Tree	replace

Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

communities

Description	Modify BGP communities attached to routes
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities
Tree	communities
Configurable	True
Platforms	Supported on all platforms

add *reference*

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.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities add <i>reference</i>
Tree	add
Reference	routing-policy community-set name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

remove *reference*

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.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> action accept bgp communities remove <i>reference</i>
Tree	remove
Reference	routing-policy community-set name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

replace *reference*

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.
Context	routing-policy policy name string statement sequence-id number action accept bgp communities replace <i>reference</i>
Tree	replace
Reference	routing-policy community-set name string
Configurable	True
Platforms	Supported on all platforms

local-preference

Description	Enter the local-preference context
Context	routing-policy policy name string statement sequence-id number action accept bgp local-preference
Tree	local-preference
Configurable	True
Platforms	Supported on all platforms

set *number*

Description	The new value of LOCAL_PREF to write into the matching BGP routes
Context	routing-policy policy name string statement sequence-id number action accept bgp local-preference set <i>number</i>
Tree	set
Configurable	True
Platforms	Supported on all platforms

origin

Description	Enter the origin context
Context	routing-policy policy name string statement sequence-id number action accept bgp origin
Tree	origin
Configurable	True

Platforms Supported on all platforms

set keyword

Description The new value of the ORIGIN attribute to write into the matching BGP routes

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [action](#)
[accept bgp origin set](#) *keyword*

Tree [set](#)

Options

- igp
- egp
- incomplete

Configurable True

Platforms Supported on all platforms

reject

Description Reject action

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [action](#) [reject](#)

Tree [reject](#)

Configurable True

Platforms Supported on all platforms

match

Description Match conditions of the policy statement

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [match](#)

Tree [match](#)

Configurable True

Platforms Supported on all platforms

bgp

Description Top-level container

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [match](#) [bgp](#)

Tree [bgp](#)

Configurable True

Platforms Supported on all platforms

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.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp as-path-length
Tree	as-path-length
Configurable	True
Platforms	Supported on all platforms

operator *keyword*

Description	The comparison operator that applies to the value
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
Default	eq
Options	<ul style="list-style-type: none"> • eq • ge • le
Configurable	True
Platforms	Supported on all platforms

unique *boolean*

Description	Count a repeated sequence of the same AS number as just 1 element
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
Default	false
Configurable	True
Platforms	Supported on all platforms

value *number*

Description	The number of (unique) AS numbers in the AS path
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
Range	0 to 255
Configurable	True
Platforms	Supported on all platforms

as-path-set *reference*

Description	Reference to an as-path-set name A route meets this condition if it matches the regular expression
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
Reference	routing-policy as-path-set name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

community-set *reference*

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
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp community-set <i>reference</i>
Tree	community-set
Reference	routing-policy community-set name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

evpn

Description	Container for match conditions that are specific to BGP EVPN routes.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp evpn
Tree	evpn
Configurable	True
Platforms	Supported on all platforms

route-type *number*

Description	An EVPN route meets this condition if the route-type field in the NLRI is one of the values provided in this list.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match bgp evpn route-type <i>number</i>
Tree	route-type
Range	1 to 5
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

family *identityref*

Description	The name of an address family A route meets this condition if the prefix belongs to the indicated address family.
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match family <i>identityref</i>
Tree	family
Options	<ul style="list-style-type: none"> • ipv4-unicast Unlabeled IPv4 unicast routes (AFI = 1, SAFI = 1) • ipv6-unicast Unlabeled IPv6 unicast routes (AFI = 2, SAFI = 1) • evpn EVPN routes (AFI = 25, SAFI = 70)
Configurable	True
Platforms	Supported on all platforms

isis

Description	Configuration for ISIS-specific policy match criteria
Context	routing-policy policy name <i>string</i> statement sequence-id <i>number</i> match isis
Tree	isis
Configurable	True
Platforms	Supported on all platforms

level number

Description	IS-IS route level
Context	routing-policy policy name string statement sequence-id number match isis level number
Tree	level
Range	1 to 2
Configurable	True
Platforms	Supported on all platforms

route-type keyword

Description	An IS-IS IPv4 prefix is external if it is signalled in TLV 130 or TLV135 with RFC 7794 X flag=1. An IS-IS IPv6 prefix is external if the TLV 236/TLV 237 external bit = 1.
Context	routing-policy policy name string statement sequence-id number match isis route-type keyword
Tree	route-type
Options	<ul style="list-style-type: none"> • internal • external
Configurable	True
Platforms	Supported on all platforms

ospf

Description	Configuration for OSPF-specific policy match criteria
Context	routing-policy policy name string statement sequence-id number match ospf
Tree	ospf
Configurable	True
Platforms	Supported on all platforms

area-id

Description	The area identifier as a dotted-quad.
Context	routing-policy policy name string statement sequence-id number match ospf area-id
Tree	area-id
Configurable	True

Platforms Supported on all platforms

instance-id *number*

Description OSPFv3 instance identifier

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [match ospf instance-id](#) *number*

Tree [instance-id](#)

Range 0 to 255

Configurable True

Platforms Supported on all platforms

route-type *identityref*

Description The OSPF route type.

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [match ospf route-type](#) *identityref*

Tree [route-type](#)

- Options**
- [type-1-ext](#)
The route has path-type type 1 external
 - [type-2-ext](#)
The route has path-type type 2 external

Configurable True

Platforms Supported on all platforms

prefix-set *reference*

Description Reference to a prefix set name

Context [routing-policy policy name](#) *string* [statement sequence-id](#) *number* [match prefix-set](#) *reference*

Tree [prefix-set](#)

Reference [routing-policy prefix-set name](#) *string*

Configurable True

Platforms Supported on all platforms

protocol *identityref*

Description	The route type to match
Context	routing-policy policy name string statement sequence-id number match protocol <i>identityref</i>
Tree	protocol
Options	<ul style="list-style-type: none"> • aggregate Locally configured aggregate route • arp-nd IP route added by ARP ND. • bgp Border Gateway Protocol version 4 • bgp-evpn BGP Ethernet VPN (EVPN) • dhcp IP (default) route added by DHCP. • gribi A gRIBI route • host A host route • isis IS-IS • local A directly connected route • linux IP route added by the linux kernel. • ndk1 Route added by an agent application using the NDK • ndk2 Route added by an agent application using the NDK • ospfv2 OSPFv2 • ospfv3 OSPFv3 • static Locally configured static route
Configurable	True

Platforms Supported on all platforms

prefix-set *name string*

Description List of defined prefix sets
Context [routing-policy prefix-set name string](#)
Tree [prefix-set](#)
Configurable True
Platforms Supported on all platforms

name *string*

Description A name used to identify the prefix set
Context [routing-policy prefix-set name string](#)
String Length 1 to 255
Configurable True
Platforms Supported on all platforms

prefix [ip-prefix \(ipv4-prefix | ipv6-prefix\)](#) [mask-length-range string](#)

Description List of prefixes in the prefix set
Context [routing-policy prefix-set name string prefix ip-prefix \(ipv4-prefix | ipv6-prefix\) mask-length-range string](#)
Tree [prefix](#)
Configurable True
Platforms Supported on all platforms

ip-prefix *(ipv4-prefix | ipv6-prefix)*

Description The IPv4 or IPv6 prefix in CIDR notation
Context [routing-policy prefix-set name string prefix ip-prefix \(ipv4-prefix | ipv6-prefix\) mask-length-range string](#)
Configurable True
Platforms Supported on all platforms

mask-length-range *string*

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
Context	routing-policy prefix-set name <i>string</i> prefix ip-prefix (<i>ipv4-prefix</i> <i>ipv6-prefix</i>) mask-length-range <i>string</i>
Configurable	True
Platforms	Supported on all platforms

10 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
- authentication-method string
- login-time string
- priv-lvl number
- remote-host string
- service-name string
- tty-name string
- username string
+ user username string
+ password string
+ role reference
+ ssh-key string
+ authorization
+ role rolename string
+ services keyword
+ tacacs
+ priv-lvl number
+ server-group name string
+ priv-lvl-authorization boolean
+ 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
- authorization-connection-failures number
- authorization-rejects number
- authorization-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
- cgroup string
- failure-action string
- failure-threshold number
- failure-window number

```

```

- last-change string
- last-start-type keyword
- launch-command string
- oom-score-adj number
- path string
- pid number
- restricted-operations keyword
- search-command string
- state keyword
- statistics
  - restart-count number
- supported-restart-types keyword
- 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
+ mode string
- oper-state string
+ timeout number
- image string
+ bridge-table
+ mac-learning
- mac-relearn-only boolean
+ mac-limit
- maximum-entries number
- warning-threshold-pct number
- proxy-arp
- statistics
  - active-entries number
  - in-active-entries number
  - neighbor-origin origin keyword
    - active-entries number
    - in-active-entries number
    - pending-entries number
    - total-entries number
  - pending-entries number
  - total-entries number
- statistics
  - active-entries number
  - failed-entries number
  - mac-type type keyword
    - active-entries number
    - failed-entries number
    - total-entries number
  - total-entries number
+ clock
+ timezone keyword
+ configuration
+ auto-checkpoint boolean

```

```

- candidate name string
- started string
- type keyword
- username string
- checkpoint id number
- comment string
- created string
- name string
- size number
- tag string
- 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
+ role name reference
+ rule path-reference string
+ action keyword
- session id number
- exclusive boolean
- name string
- started string
- type keyword
- username string
+ dhcp-server
+ admin-state keyword
+ network-instance name reference
+ dhcpv4
+ admin-state keyword
- oper-state keyword
+ options
+ bootfile-name string
+ dns-server string
+ domain-name string
+ hostname string
+ ntp-server string
+ router string
+ server-id string
+ static-allocation
+ host mac string
+ ip-address string
+ options
+ bootfile-name string
+ dns-server string
+ domain-name string
+ hostname string
+ ntp-server string
+ router string
+ server-id string
- statistics
- client-packets-discarded number
- client-packets-received number
- server-packets-sent number
+ trace-options
+ trace keyword
+ dhcpv6
+ admin-state keyword

```

```

- oper-state keyword
+ options
+ dns-server string
+ static-allocation
+ host mac string
+ ip-address string
+ options
+ dns-server string
- statistics
- client-packets-discarded number
- client-packets-received number
- server-packets-sent number
+ trace-options
+ trace keyword
+ 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
+ commit-save boolean
+ include-defaults-in-config-only-responses boolean
+ network-instance name reference
+ admin-state keyword
- oper-state keyword
+ port number
+ source-address (ipv4-address | ipv6-address)
+ tls-profile reference
+ use-authentication boolean
+ yang-models keyword
+ 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
+ yang-models keyword
+ gribi-server
+ admin-state keyword
- client id number

```

```

- election-id string
- persistence-mode keyword
- remote-host (ipv4-address | ipv6-address)
- remote-port number
- start-time string
- user string
- user-agent string
+ 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
+ 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
- last-booted string
+ location string
- version string
+ 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
- l2cp-transparency
- l2cp-statistics
- dot1x
- in-trap-to-cpu-packets number
- in-tunneled-packets number
- last-clear string
- lacp
- in-trap-to-cpu-packets number
- in-tunneled-packets number

```

```

- last-clear string
- last-clear string
- lldp
- in-trap-to-cpu-packets number
- in-tunneled-packets number
- last-clear string
- ptp
- in-trap-to-cpu-packets number
- in-tunneled-packets number
- last-clear string
- total-in-discarded-packets number
- total-in-packets number
- total-in-trap-to-cpu-packets number
- total-in-tunneled-packets number
- xstp
- in-trap-to-cpu-packets number
- in-tunneled-packets number
- last-clear string
+ lacp
+ system-id string
+ system-priority number
+ lldp
+ admin-state keyword
- chassis-id string
- chassis-id-type keyword
+ hello-timer number
+ hold-multiplier number
+ interface name reference
+ admin-state keyword
- neighbor id string
- capability name identityref
- 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
+ load-balancing
+ hash-options
+ destination-address boolean
+ destination-port boolean
+ hash-seed number
+ ipv6-flow-label boolean
+ mpls-label-stack boolean
+ protocol boolean
+ source-address boolean
+ source-port boolean
+ vlan boolean
+ 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
  + isis
    + network-instances reference
+ profile name string
+ bgp
  + export-policy reference
  + import-policy reference
+ isis
  + overload
    + max-metric boolean
    + set-bit boolean
+ management
+ openconfig
  + admin-state keyword
  - oper-state keyword
+ mirroring
+ mirroring-instance name string
+ admin-state keyword
+ description string
+ mirror-destination
  + local string
  + remote
    + encap keyword
    + network-instance reference
    + tunnel-end-points
      + admin-state keyword
      + dst-ipv4 string
      + dst-ipv6 string
      - oper-state keyword
      + src-ipv4 string
      + src-ipv6 string
+ mirror-source
  + acl
    + ipv4-filter name reference
    + entry sequence-id reference
    + ipv6-filter name reference
    + entry sequence-id reference
  + interface name string
  + direction keyword
  + subinterface name string
  + direction keyword
- oper-down-reason keyword
- oper-state keyword

```

```

+ mtu
+ default-ip-mtu number
+ default-l2-mtu number
+ default-mpls-mtu number
+ default-port-mtu number
+ min-path-mtu number
+ name
+ domain-name string
+ host-name string
+ network-instance
+ protocols
+ bgp-vpn
+ bgp-instance id number
- oper-down-reason keyword
+ route-distinguisher
- rd (string | string | string | string)
- route-distinguisher-origin keyword
+ route-target
- export-route-target-origin keyword
- export-rt (string | string | string | string | string | string | string |
string | string | string)
- import-route-target-origin keyword
- import-rt (string | string | string | string | string | string | string |
string | string | string)
+ evpn
+ ethernet-segments
+ bgp-instance id reference
+ ethernet-segment name string
+ admin-state keyword
- association
- network-instance name string
- bgp-instance instance number
- computed-designated-forwarder-candidates
- designated-forwarder-candidate address (ipv4-address | ipv6-
address)
- add-time string
- designated-forwarder boolean
- designated-forwarder-activation-start-time string
- designated-forwarder-activation-time number
- designated-forwarder-role-last-change string
- autodiscovery-per-ethernet-segment-routes
- attr-id reference
- esi string
- ethernet-tag-id number
- neighbor (ipv4-address | ipv6-address)
- route-distinguisher (string | string | string | string)
- vni number
+ df-election
+ algorithm
+ manual-alg
+ primary-evi-range start-evi number
+ end-evi number
- oper-type keyword
+ preference-alg
+ capabilities
+ ac-df keyword
+ non-revertive boolean
- oper-do-not-preempt boolean
- oper-preference-value number
+ preference-value number
+ type keyword
+ interface-standby-signaling-on-non-df
+ timers
+ activation-timer number
+ esi string
- ethernet-segment-routes

```

```

- attr-id reference
- esi string
- neighbor (ipv4-address | ipv6-address)
- originating-router (ipv4-address | ipv6-address)
- route-distinguisher (string | string | string | string)
+ interface ethernet-interface reference
+ multi-homing-mode keyword
+ next-hop l3-next-hop (ipv4-address | ipv6-address)
+ evi start number
- oper-down-reason keyword
- oper-esi string
- oper-multi-homing-mode keyword
- oper-state keyword
+ routes
+ ethernet-segment
+ originating-ip keyword
+ next-hop keyword
+ type keyword
+ timers
+ activation-timer number
- boot-remaining-time number
- boot-start-time string
+ boot-timer number
+ 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)
+ ra-guard-policy name string
+ action keyword
+ advertise-prefix-set reference
+ hop-limit number
+ managed-config-flag boolean
+ other-config-flag boolean
+ router-preference keyword
+ source-prefix-set reference
+ 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
+ warm-reboot
+ bgp-max-wait number
```

10.1 system Descriptions

system

Description	Enclosing container for system management
Context	system
Tree	system
Configurable	True
Platforms	Supported on all platforms

aaa

Description	Top-level container for AAA services
Context	system aaa
Tree	aaa
Configurable	True
Platforms	Supported on all platforms

accounting

Description	Top-level container for accounting
Context	system aaa accounting
Tree	accounting
Configurable	True
Platforms	Supported on all platforms

accounting-method *reference*

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.
Context	system aaa accounting accounting-method <i>reference</i>
Tree	accounting-method
Reference	system aaa server-group name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

event *event-type identityref*

Description	List of events subject to accounting
Context	system aaa accounting event event-type identityref
Tree	event
Configurable	True
Platforms	Supported on all platforms

event-type *identityref*

Description	The type of activity to record at the accounting server
Context	system aaa accounting event event-type identityref
Options	<ul style="list-style-type: none"> command Specifies interactive command events for AAA accounting
Configurable	True
Platforms	Supported on all platforms

record *identityref*

Description	Type of record to send to the accounting server for this activity type
Context	system aaa accounting event event-type identityref record identityref
Tree	record
Options	<ul style="list-style-type: none"> start-stop Send start and stop records for user activities 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 Send only stop records for user activities A stop record is sent to the accounting server when the user activity completes
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Top-level container for global authentication data
--------------------	--

Context	system aaa authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

admin-user

Description	Enclosing container for admin user
Context	system aaa authentication admin-user
Tree	admin-user
Configurable	True
Platforms	Supported on all platforms

password *string*

Description	The admin password, supplied as cleartext The system will hash the value, storing only the hashed value
Context	system aaa authentication admin-user password <i>string</i>
Tree	password
Configurable	True
Platforms	Supported on all platforms

username *string*

Description	Assigned username for admin user
Context	system aaa authentication admin-user username <i>string</i>
Tree	username
Default	admin
Configurable	False
Platforms	Supported on all platforms

authentication-method *reference*

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.
--------------------	---

Context	system aaa authentication authentication-method <i>reference</i>
Tree	authentication-method
Reference	system aaa server-group name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

exit-on-reject *boolean*

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.
Context	system aaa authentication exit-on-reject <i>boolean</i>
Tree	exit-on-reject
Default	false
Configurable	True
Platforms	Supported on all platforms

idle-timeout *number*

Description	Set the idle timeout of all CLI sessions After the timeout is reached, the session is disconnected from the system.
Context	system aaa authentication idle-timeout <i>number</i>
Tree	idle-timeout
Default	600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

session id *number*

Description	List of active sessions in the system
Context	system aaa authentication session id <i>number</i>
Tree	session
Configurable	False
Platforms	Supported on all platforms

id number

Description	System generated session ID
Context	system aaa authentication session id number
Configurable	False
Platforms	Supported on all platforms

authentication-method string

Description	Authentication method that authorized the user (the server-group name or local)
Context	system aaa authentication session id number authentication-method string
Tree	authentication-method
Configurable	False
Platforms	Supported on all platforms

login-time string

Description	Time the user logged in
Context	system aaa authentication session id number login-time string
Tree	login-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

priv-lvl number

Description	TACACS+ authorization priv-lvl (if TACACS+ authorization is enabled)
Context	system aaa authentication session id number priv-lvl number
Tree	priv-lvl
Configurable	False
Platforms	Supported on all platforms

remote-host string

Description	Remote host of the session
Context	system aaa authentication session id number remote-host string

Tree	remote-host
Configurable	False
Platforms	Supported on all platforms

service-name *string*

Description	Service name that called login for the session
Context	system aaa authentication session id number service-name <i>string</i>
Tree	service-name
Configurable	False
Platforms	Supported on all platforms

tty-name *string*

Description	Terminal type
Context	system aaa authentication session id number tty-name <i>string</i>
Tree	tty-name
Configurable	False
Platforms	Supported on all platforms

username *string*

Description	Username linked to the session
Context	system aaa authentication session id number username <i>string</i>
Tree	username
Configurable	False
Platforms	Supported on all platforms

user [username](#) *string*

Description	List of local users configured on the system
Context	system aaa authentication user username <i>string</i>
Tree	user
Configurable	True
Platforms	Supported on all platforms
Max. Elements	128

username *string*

Description	Assigned username for this user
Context	system aaa authentication user username <i>string</i>
String Length	1 to 32
Configurable	True
Platforms	Supported on all platforms

password *string*

Description	The user password, supplied as cleartext The system will hash the value on input, storing only the hashed value
Context	system aaa authentication user username <i>string password</i> <i>string</i>
Tree	password
Configurable	True
Platforms	Supported on all platforms

role *reference*

Description	List of roles to assign to this user The most specific rule for a particular role takes precedence. Rules from all user roles are evaluated together, most permissive privilege taking precedence.
Context	system aaa authentication user username <i>string role</i> <i>reference</i>
Tree	role
Reference	system aaa authorization role rolename <i>string</i>
Configurable	True
Platforms	Supported on all platforms
Max. Elements	32

ssh-key *string*

Description	SSH public key(s) for the user (RSA) If defined, the user may login to the system over SSH with this key. This field includes the 'ssh-rsa' leader, as would normally be found in a SSH key.
Context	system aaa authentication user username <i>string ssh-key</i> <i>string</i>
Tree	ssh-key

Configurable	True
Platforms	Supported on all platforms
Max. Elements	32

authorization

Description	Top-level container for authorization configuration and operational state data
Context	system aaa authorization
Tree	authorization
Configurable	True
Platforms	Supported on all platforms

role [rolename string](#)

Description	List of local roles configured on the system
Context	system aaa authorization role rolename string
Tree	role
Configurable	True
Platforms	Supported on all platforms

rolename [string](#)

Description	Assigned rolename for this role
Context	system aaa authorization role rolename string
String Length	1 to 32
Configurable	True
Platforms	Supported on all platforms

services [keyword](#)

Description	Services that members of this role are authorized for Services are additive, if a user is a member of multiple roles, the available services are merged.
Context	system aaa authorization role rolename string services keyword
Tree	services
Options	<ul style="list-style-type: none"> cli gnmi

- gribi
- p4rt
- json-rpc
- ftp

Configurable	True
Platforms	Supported on all platforms

tacacs

Description	Top-level container for configuration relating to TACACS+ interworking with roles
Context	system aaa authorization role rolename string tacacs
Tree	tacacs
Configurable	True
Platforms	Supported on all platforms

priv-lvl *number*

Description	The TACACS+ priv-lvl to map to this role All roles matching each specific priv-lvl, and their lessers are merged together to create the final ruleset applied to the user.
Context	system aaa authorization role rolename string tacacs priv-lvl number
Tree	priv-lvl
Range	0 to 15
Configurable	True
Platforms	Supported on all platforms

server-group *name string*

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.
Context	system aaa server-group name string
Tree	server-group
Configurable	True
Platforms	Supported on all platforms
Max. Elements	2

name *string*

Description	User defined name for the server group
Context	system aaa server-group name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

priv-lvl-authorization *boolean*

Description	Use TACACS+ priv-lvl based authorization If false, then authorization is skipped for TACACS+ users granting full admin access for those users.
Context	system aaa server-group name <i>string</i> priv-lvl-authorization <i>boolean</i>
Tree	priv-lvl-authorization
Default	false
Configurable	True
Platforms	Supported on all platforms

server [address](#) (*ipv4-address* | *ipv6-address*)

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
Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	5

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

Description	Address used to reach the server
Context	system aaa server-group name <i>string</i> server address (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	True

Platforms Supported on all platforms

name *string*

Description User defined name assigned to the server

Context [system aaa server-group name string server address \(ipv4-address | ipv6-address\) name string](#)

Tree [name](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

network-instance *reference*

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 difference network-instances for connectivity.

Context [system aaa server-group name string server address \(ipv4-address | ipv6-address\) network-instance reference](#)

Tree [network-instance](#)

Reference [network-instance name string](#)

Configurable True

Platforms Supported on all platforms

oper-state *keyword*

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.

Context [system aaa server-group name string server address \(ipv4-address | ipv6-address\) oper-state keyword](#)

Tree [oper-state](#)

- 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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

statistics**Description**

Enclosing container for server statistics

Context[system aaa server-group name string server address \(ipv4-address | ipv6-address\) statistics](#)**Tree**[statistics](#)

Configurable	False
Platforms	Supported on all platforms

accounting-connection-failures *number*

Description	Number of accounting connection failures
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics accounting-connection-failures number
Tree	accounting-connection-failures
Default	0
Configurable	False
Platforms	Supported on all platforms

accounting-rejects *number*

Description	Number of accounting rejections
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics accounting-rejects number
Tree	accounting-rejects
Default	0
Configurable	False
Platforms	Supported on all platforms

accounting-success *number*

Description	Number of accounting successes
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics accounting-success number
Tree	accounting-success
Default	0
Configurable	False
Platforms	Supported on all platforms

authorization-connection-failures *number*

Description	Number of authorization connection failures
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics authorization-connection-failures number

Tree	authorization-connection-failures
Default	0
Configurable	False
Platforms	Supported on all platforms

authorization-rejects *number*

Description	Number of authorization rejections
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics authorization-rejects number
Tree	authorization-rejects
Default	0
Configurable	False
Platforms	Supported on all platforms

authorization-success *number*

Description	Number of authorization successes
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics authorization-success number
Tree	authorization-success
Default	0
Configurable	False
Platforms	Supported on all platforms

login-connection-failures *number*

Description	Number of login connection failures
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics login-connection-failures number
Tree	login-connection-failures
Default	0
Configurable	False
Platforms	Supported on all platforms

login-rejects *number*

Description	Number of login rejections
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics login-rejects number
Tree	login-rejects
Default	0
Configurable	False
Platforms	Supported on all platforms

login-success *number*

Description	Number of login successes
Context	system aaa server-group name string server address (ipv4-address ipv6-address) statistics login-success number
Tree	login-success
Default	0
Configurable	False
Platforms	Supported on all platforms

tacacs

Description	Top-level container for TACACS+ server data
Context	system aaa server-group name string server address (ipv4-address ipv6-address) tacacs
Tree	tacacs
Configurable	True
Platforms	Supported on all platforms

port *number*

Description	The port number on which to contact the TACACS+ server
Context	system aaa server-group name string server address (ipv4-address ipv6-address) tacacs port number
Tree	port
Range	0 to 65535
Default	49
Configurable	True

Platforms Supported on all platforms

secret-key string

Description The unencrypted shared key used between the system and server

Context [system aaa server-group name string server address \(ipv4-address | ipv6-address\) tacacs secret-key string](#)

Tree [secret-key](#)

Configurable True

Platforms Supported on all platforms

timeout number

Description Set the timeout in seconds on responses from servers in this group

Context [system aaa server-group name string timeout number](#)

Tree [timeout](#)

Range 1 to 3600

Default 10

Units seconds

Configurable True

Platforms Supported on all platforms

type identityref

Description AAA server type -- all servers in the group must be of this type

Context [system aaa server-group name string type identityref](#)

Tree [type](#)

Options

- tacacs
 - Specifies servers using the TACACS+ protocol
 - Specifies servers using the TACACS+ protocol Terminal Access Controller Access Control System (TACACS+)
- local
 - Specifies using Linux local methods
 - Specifies using Linux local methods This type cannot be combined with a server address

Configurable True

Platforms Supported on all platforms

app-management

Description	Top-level container for application configuration and state
Context	system app-management
Tree	app-management
Configurable	False
Platforms	Supported on all platforms

application name string

Description	List of all applications managed by the application manager
Context	system app-management application name string
Tree	application
Configurable	False
Platforms	Supported on all platforms

name string

Description	Unique name of this application instance
Context	system app-management application name string
Configurable	False
Platforms	Supported on all platforms

author string

Description	The author of the application
Context	system app-management application name string author string
Tree	author
Configurable	False
Platforms	Supported on all platforms

cgroup string

Description	Cgroup in with this application is started
Context	system app-management application name string cgroup string
Tree	cgroup

Configurable	False
Platforms	Supported on all platforms

failure-action *string*

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
Context	system app-management application name <i>string</i> failure-action <i>string</i>
Tree	failure-action
Configurable	False
Platforms	Supported on all platforms

failure-threshold *number*

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
Context	system app-management application name <i>string</i> failure-threshold <i>number</i>
Tree	failure-threshold
Range	0 to 255
Configurable	False
Platforms	Supported on all platforms

failure-window *number*

Description	Sliding window in seconds, over which to count restarts towards failure-threshold
Context	system app-management application name <i>string</i> failure-window <i>number</i>
Tree	failure-window
Range	300 to 86400
Units	seconds
Configurable	False
Platforms	Supported on all platforms

last-change *string*

Description	Date and time the application instance last changed state
Context	system app-management application name <i>string last-change string</i>
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-start-type *keyword*

Description	Indicates the type of the most recent start or restart of this application instance
Context	system app-management application name <i>string last-start-type keyword</i>
Tree	last-start-type
Options	<ul style="list-style-type: none"> • warm A warm start indicates that the application will leave state in IDB during a restart, and recover it post restart A warm start indicates that the application will leave state in IDB during a restart, and recover it post restart This type results in less disruption to surrounding applications and functionality. • cold A cold start indicates that the application will not leave state in IDB during a restart A cold start indicates that the application will not leave state in IDB during a restart This type is equivalent to a normal application restart, i.e. one where the application's state is purged from the system during the restart, and recreated after.
Configurable	False
Platforms	Supported on all platforms

launch-command *string*

Description	The command used to launch the application
Context	system app-management application name <i>string launch-command string</i>
Tree	launch-command
Configurable	False
Platforms	Supported on all platforms

oom-score-adj *number*

Description	OOM score adj value set for this application
Context	system app-management application name <i>string</i> oom-score-adj <i>number</i>
Tree	oom-score-adj
Configurable	False
Platforms	Supported on all platforms

path *string*

Description	The directory where the application can be found
Context	system app-management application name <i>string</i> path <i>string</i>
Tree	path
Configurable	False
Platforms	Supported on all platforms

pid *number*

Description	Process ID of this application instance
Context	system app-management application name <i>string</i> pid <i>number</i>
Tree	pid
Configurable	False
Platforms	Supported on all platforms

restricted-operations *keyword*

Description	The operations that may not be manually performed on this application
Context	system app-management application name <i>string</i> restricted-operations <i>keyword</i>
Tree	restricted-operations
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

	<ul style="list-style-type: none"> quit This application may not be terminated manually kill This application may not be terminated ungracefully manually
Configurable	False
Platforms	Supported on all platforms

search-command *string*

Description	The command used to search for the applications liveness
Context	system app-management application name string search-command string
Tree	search-command
Configurable	False
Platforms	Supported on all platforms

state *keyword*

Description	Current state of this application instance
Context	system app-management application name string state keyword
Tree	state
Options	<ul style="list-style-type: none"> running Application instance is 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 Application instance is loaded, but has no configuration This state requires wait-for-config true within the applications YAML configuration. This results in the application being loaded into app-mgr, but not starting until the system receives configuration for it error The application has not started successfully, or has failed 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 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

The application is not running This state is most likely caused by an operator action

Configurable

False

Platforms

Supported on all platforms

statistics

Description

Top-level container for application statistics

Context

[system app-management application name](#) *string* [statistics](#)

Tree

[statistics](#)

Configurable

False

Platforms

Supported on all platforms

restart-count *number*

Description

The number of times this application instance has restarted

Context

[system app-management application name](#) *string* [statistics](#) [restart-count](#) *number*

Tree

[restart-count](#)

Default

0

Configurable

False

Platforms

Supported on all platforms

supported-restart-types *keyword*

Description

Indicates the supported restart types for this application

Context

[system app-management application name](#) *string* [supported-restart-types](#) *keyword*

Tree

[supported-restart-types](#)

Options

- warm

A warm start indicates that the application will leave state in IDB during a restart, and recover it post restart

A warm start indicates that the application will leave state in IDB during a restart, and recover it post restart This type results in less disruption to surrounding applications and functionality.

- cold

A cold start indicates that the application will not leave state in IDB during a restart

A cold start indicates that the application will not leave state in IDB during a restart This type is equivalent to a normal application restart, i.e. one where the application's state is purged from the system during the restart, and recreated after.

Configurable

False

Platforms

Supported on all platforms

version string

Description

The version of the application

Context

[system app-management application name string version string](#)

Tree

[version](#)

Configurable

False

Platforms

Supported on all platforms

yang

Description

Top-level container for application state related to YANG

Context

[system app-management application name string yang](#)

Tree

[yang](#)

Configurable

False

Platforms

Supported on all platforms

modules string

Description

YANG module names used by this application instance

Context

[system app-management application name string yang modules string](#)

Tree

[modules](#)

Configurable

False

Platforms

Supported on all platforms

source-directories *string*

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
Context	system app-management application name <i>string</i> yang source-directories <i>string</i>
Tree	source-directories
Configurable	False
Platforms	Supported on all platforms

authentication

Description	Container for protocol authentication options available system wide
Context	system authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

keychain [name](#) *string*

Description	List of system keychains
Context	system authentication keychain name <i>string</i>
Tree	keychain
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1024

name *string*

Description	The user configured name for the keychain
Context	system authentication keychain name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

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/or all inbound messages with authentication data are dropped, depending on the context. A keychain is operationally disabled in a particular direction (send/receive) if:
Context	system authentication keychain name <i>string</i> admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

description *string*

Description	The user configured description for the keychain
Context	system authentication keychain name <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

key *index number*

Description	List of keys in the keychain
Context	system authentication keychain name <i>string</i> key <i>index number</i>
Tree	key
Configurable	True
Platforms	Supported on all platforms

index *number*

Description	Each key in a keychain requires a unique identifier. The index value specifies this identifier.
Context	system authentication keychain name <i>string</i> key <i>index number</i>
Configurable	True

Platforms Supported on all platforms

algorithm *keyword*

Description The cryptographic algorithm used with the keying material to secure the messages.

Context [system authentication keychain name](#) *string* [key index number](#) [algorithm keyword](#)

Tree [algorithm](#)

Options

- **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

Platforms Supported on all platforms

authentication-key *string*

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.

Context	system authentication keychain name <i>string</i> key index number <i>authentication-key</i> <i>string</i>
Tree	authentication-key
String Length	1 to 25
Configurable	True
Platforms	Supported on all platforms

type *keyword*

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.
Context	system authentication keychain name <i>string</i> type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • 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. • vrrp Keychain intended to be used for authentication of VRRPv2 messages.
Configurable	True
Platforms	Supported on all platforms

banner

Description	Contains configuration and state related to system banners
Context	system banner
Tree	banner
Configurable	True
Platforms	Supported on all platforms

login-banner *string*

Description	Banner to display before a user has authenticated
Context	system banner login-banner <i>string</i>
Tree	login-banner
Configurable	True
Platforms	Supported on all platforms

motd-banner *string*

Description	Banner to display after a user has authenticated
Context	system banner motd-banner <i>string</i>
Tree	motd-banner
Configurable	True
Platforms	Supported on all platforms

boot

Description	Top-level container for configuration and state data related to booting the system
Context	system boot
Tree	boot
Configurable	True
Platforms	Supported on all platforms

autoboot

Description	Top-level container for configuration and state data related to autobooting the system
Context	system boot autoboot
Tree	autoboot
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable autoboot functionality
Context	system boot autoboot admin-state <i>keyword</i>

Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

attempts *number*

Description	Sets the amount of executions to try autoboot, before rebooting the system
Context	system boot autoboot attempts <i>number</i>
Tree	attempts
Range	1 to 10
Configurable	True
Platforms	Supported on all platforms

client-id *keyword*

Description	The client ID to use on outgoing DHCP requests
Context	system boot autoboot client-id <i>keyword</i>
Tree	client-id
Options	<ul style="list-style-type: none"> • serial Use the chassis serial number as the client ID
Configurable	True
Platforms	Supported on all platforms

interface *reference*

Description	Sets the interface to use for autoboot functionality
Context	system boot autoboot interface <i>reference</i>
Tree	interface
Default	mgmt0
Reference	interface name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

mode *string*

Description	Ztp operation modes. One or more modes can be passed
Context	system boot autoboot mode <i>string</i>
Tree	mode
Configurable	True
Platforms	Supported on all platforms

oper-state *string*

Description	The current operational status of the autoboot process
Context	system boot autoboot oper-state <i>string</i>
Tree	oper-state
Configurable	False
Platforms	Supported on all platforms

timeout *number*

Description	Sets the timeout for each attempt to autoboot
Context	system boot autoboot timeout <i>number</i>
Tree	timeout
Range	200 to 3600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

image *string*

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/nokiaos/<folder>
Context	system boot image <i>string</i>
Tree	image
String Length	1 to 255
Configurable	False

Platforms	Supported on all platforms
Max. Elements	3

bridge-table

Description	system bridge-table information
Context	system bridge-table
Tree	bridge-table
Configurable	True
Platforms	Supported on all platforms

mac-learning

Description	Enter the mac-learning context
Context	system bridge-table mac-learning
Tree	mac-learning
Configurable	True
Platforms	Supported on all platforms

mac-relearn-only *boolean*

Description	The value of this leaf indicates that the system will not learn any new mac addresses, but will relearn any that are already programmed
Context	system bridge-table mac-learning mac-relearn-only boolean
Tree	mac-relearn-only
Configurable	False
Platforms	Supported on all platforms

mac-limit

Description	Bridge Table size and thresholds.
Context	system bridge-table mac-limit
Tree	mac-limit
Configurable	True
Platforms	Supported on all platforms

maximum-entries *number*

Description	Maximum number of mac addresses allowed in the system bridge-table.
Context	system bridge-table mac-limit maximum-entries number
Tree	maximum-entries
Configurable	False
Platforms	Supported on all platforms

warning-threshold-pct *number*

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%
Context	system bridge-table mac-limit warning-threshold-pct number
Tree	warning-threshold-pct
Configurable	False
Platforms	Supported on all platforms

proxy-arp

Description	system bridge-table proxy ARP information
Context	system bridge-table proxy-arp
Tree	proxy-arp
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	system bridge-table proxy-arp statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-entries *number*

Description	The total number of active proxy ARP entries.
Context	system bridge-table proxy-arp statistics active-entries number

Tree	active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

in-active-entries *number*

Description	The total number of inactive proxy ARP entries.
Context	system bridge-table proxy-arp statistics in-active-entries <i>number</i>
Tree	in-active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

neighbor-origin [origin](#) *keyword*

Description	the origin of the proxy ARP installed in the table.
Context	system bridge-table proxy-arp statistics neighbor-origin origin <i>keyword</i>
Tree	neighbor-origin
Configurable	False
Platforms	Supported on all platforms

origin *keyword*

Description	Enter the origin context
Context	system bridge-table proxy-arp statistics neighbor-origin origin <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • dynamic • evpn • duplicate
Configurable	False
Platforms	Supported on all platforms

active-entries *number*

Description	The total number of active proxy ARP entries.
--------------------	---

Context	system bridge-table proxy-arp statistics neighbor-origin origin <i>keyword active-entries number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

in-active-entries *number*

Description	The total number of inactive proxy ARP entries.
Context	system bridge-table proxy-arp statistics neighbor-origin origin <i>keyword in-active-entries number</i>
Tree	in-active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

pending-entries *number*

Description	The total number of pending proxy ARP entries.
Context	system bridge-table proxy-arp statistics neighbor-origin origin <i>keyword pending-entries number</i>
Tree	pending-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

total-entries *number*

Description	The total number of proxy ARP entries.
Context	system bridge-table proxy-arp statistics neighbor-origin origin <i>keyword total-entries number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

pending-entries *number*

Description	The total number of pending proxy ARP entries.
Context	system bridge-table proxy-arp statistics pending-entries <i>number</i>
Tree	pending-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

total-entries *number*

Description	The total number of proxy ARP entries.
Context	system bridge-table proxy-arp statistics total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	system bridge-table statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

active-entries *number*

Description	The total number of macs that are active on the system.
Context	system bridge-table statistics active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

failed-entries *number*

Description	The total number of macs, which have not been programmed on atleast one slot
Context	system bridge-table statistics failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

mac-type *type keyword*

Description	the type of the mac in the system.
Context	system bridge-table statistics mac-type type <i>keyword</i>
Tree	mac-type
Configurable	False
Platforms	Supported on all platforms

type *keyword*

Description	Enter the type context
Context	system bridge-table statistics mac-type type <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe
Configurable	False
Platforms	Supported on all platforms

active-entries *number*

Description	The total number of macs of this type on the system.
Context	system bridge-table statistics mac-type type keyword active-entries number
Tree	active-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

failed-entries *number*

Description	The total number of macs of this type, which have not been programmed on atleast one slot
Context	system bridge-table statistics mac-type type keyword failed-entries number
Tree	failed-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

total-entries *number*

Description	The total number of macs of this type , active and inactive, on the system.
Context	system bridge-table statistics mac-type type keyword total-entries number
Tree	total-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

total-entries *number*

Description	The total number of macs, active and inactive, on the system.
Context	system bridge-table statistics total-entries number
Tree	total-entries
Default	0
Configurable	False
Platforms	Supported on all platforms

clock

Description	Top-level container for system clock configuration and state
Context	system clock
Tree	clock
Configurable	True
Platforms	Supported on all platforms

timezone *keyword*

Description	The timezone to use for the system Based on IANAs Time Zone database
Context	system clock timezone <i>keyword</i>
Tree	timezone
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); Malukus/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
Platforms	Supported on all platforms

configuration

Description	Top-level container for configuration and state data related to the system configuration
Context	system configuration
Tree	configuration
Configurable	True
Platforms	Supported on all platforms

auto-checkpoint *boolean*

Description	Configuration checkpoint will be automatically created after every successful commit (if set to true).
Context	system configuration auto-checkpoint <i>boolean</i>
Tree	auto-checkpoint

Default	false
Configurable	True
Platforms	Supported on all platforms

candidate *name string*

Description	List of configuration candidates currently active
Context	system configuration candidate name string
Tree	candidate
Configurable	False
Platforms	Supported on all platforms

name *string*

Description	Name of the configuration candidate
Context	system configuration candidate name string
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

started *string*

Description	Start date and time of the configuration session
Context	system configuration candidate name string started string
Tree	started
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

type *keyword*

Description	Type of configuration candidate
Context	system configuration candidate name string type keyword
Tree	type
Options	<ul style="list-style-type: none"> • shared • private

Configurable	False
Platforms	Supported on all platforms

username *string*

Description	User that started the configuration session
Context	system configuration candidate name <i>string</i> username <i>string</i>
Tree	username
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

checkpoint id *number*

Description	List of current checkpoints present in the system
Context	system configuration checkpoint id <i>number</i>
Tree	checkpoint
Configurable	False
Platforms	Supported on all platforms

id *number*

Description	System generated ID for the checkpoint
Context	system configuration checkpoint id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

comment *string*

Description	User provided annotations associated with the checkpoint
Context	system configuration checkpoint id <i>number</i> comment <i>string</i>
Tree	comment
Configurable	False
Platforms	Supported on all platforms

created *string*

Description	Date and time this checkpoint was created
Context	system configuration checkpoint id <i>number</i> created <i>string</i>
Tree	created
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

name *string*

Description	User provided name of the checkpoint
Context	system configuration checkpoint id <i>number</i> name <i>string</i>
Tree	name
Configurable	False
Platforms	Supported on all platforms

size *number*

Description	Size of the checkpoint configuration file
Context	system configuration checkpoint id <i>number</i> size <i>number</i>
Tree	size
Units	bytes
Configurable	False
Platforms	Supported on all platforms

tag *string*

Description	Full system version that the checkpoint was generated on
Context	system configuration checkpoint id <i>number</i> tag <i>string</i>
Tree	tag
Configurable	False
Platforms	Supported on all platforms

username *string*

Description	Username that created this checkpoint
--------------------	---------------------------------------

Context	system configuration checkpoint id <i>number</i> username <i>string</i>
Tree	username
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

version *string*

Description	System version that the checkpoint was generated on
Context	system configuration checkpoint id <i>number</i> version <i>string</i>
Tree	version
Configurable	False
Platforms	Supported on all platforms

commit *id number*

Description	List of configuration transactions
Context	system configuration commit id <i>number</i>
Tree	commit
Configurable	False
Platforms	Supported on all platforms

id *number*

Description	System identifier for the commit
Context	system configuration commit id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

comment *string*

Description	Operator provided comment associated with this commit
Context	system configuration commit id <i>number</i> comment <i>string</i>
Tree	comment
Configurable	False
Platforms	Supported on all platforms

ended string

Description	End date and time of the commit This field is not populated if the commit is in progress
Context	system configuration commit id number ended string
Tree	ended
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

name string

Description	Name of the configuration candidate the commit was triggered from
Context	system configuration commit id number name string
Tree	name
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

started string

Description	Start date and time of the commit
Context	system configuration commit id number started string
Tree	started
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

status keyword

Description	Current status of the commit
Context	system configuration commit id number status keyword
Tree	status
Options	<ul style="list-style-type: none"> • validating • publishing • unconfirmed

- checkpoint
- save
- complete
- reverting
- failed

Configurable

False

Platforms

Supported on all platforms

type *keyword***Description**

Type of configuration candidate the commit was triggered from

Context[system configuration commit id](#) *number type keyword***Tree**[type](#)**Options**

- shared
- private

Configurable

False

Platforms

Supported on all platforms

username *string***Description**

User that started the commit

Context[system configuration commit id](#) *number username string***Tree**[username](#)**String Length**

1 to 255

Configurable

False

Platforms

Supported on all platforms

idle-timeout *number***Description**

The idle timeout of configuration candidates

After this period of no activity, the candidate is emptied and removed from the system.

Context[system configuration idle-timeout](#) *number***Tree**[idle-timeout](#)**Default**

10080

Units

minutes

Configurable	True
Platforms	Supported on all platforms

last-change *string*

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.
Context	system configuration last-change string
Tree	last-change
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

max-candidates *number*

Description	The maximum number of combined private and shared candidates
Context	system configuration max-candidates number
Tree	max-candidates
Range	1 to 255
Default	10
Configurable	True
Platforms	Supported on all platforms

max-checkpoints *number*

Description	The number of checkpoints kept by the system
Context	system configuration max-checkpoints number
Tree	max-checkpoints
Range	1 to 255
Default	10
Configurable	True
Platforms	Supported on all platforms

role *name reference*

Description	List of roles configured in the system
--------------------	--

Context	system configuration role name <i>reference</i>
Tree	role
Configurable	True
Platforms	Supported on all platforms
Max. Elements	32

name *reference*

Description	Enter the name context
Context	system configuration role name <i>reference</i>
Reference	system aaa authorization role rolename <i>string</i>
Configurable	True
Platforms	Supported on all platforms

rule [path-reference](#) *string*

Description	List of paths to perform access control against
Context	system configuration role name <i>reference</i> rule path-reference <i>string</i>
Tree	rule
Configurable	True
Platforms	Supported on all platforms
Max. Elements	256

path-reference *string*

Description	Reference to a valid YANG path, in CLI notation This path may include keys, wildcards, ranges, and other management server supported constructs. Ranges will be expanded. The root path can be specified with '/'. E.g. / "/interface" "/acl ipv4-filter foo* description"
Context	system configuration role name <i>reference</i> rule path-reference <i>string</i>
Configurable	True
Platforms	Supported on all platforms

action *keyword*

Description	Action to allow for this path
--------------------	-------------------------------

Context	system configuration role name <i>reference</i> rule path-reference <i>string</i> action keyword
Tree	action
Options	<ul style="list-style-type: none"> • read This path may be read by the role • write This path may be written and read by the role • deny This path may not be read or written to by the role
Configurable	True
Platforms	Supported on all platforms

session id *number*

Description	List of configuration sessions currently active
Context	system configuration session id <i>number</i>
Tree	session
Configurable	False
Platforms	Supported on all platforms

id *number*

Description	System generated ID for the configuration session
Context	system configuration session id <i>number</i>
Configurable	False
Platforms	Supported on all platforms

exclusive *boolean*

Description	Details if this session is running in exclusive mode
Context	system configuration session id <i>number</i> exclusive <i>boolean</i>
Tree	exclusive
Configurable	False
Platforms	Supported on all platforms

name *string*

Description	Name of the candidate the session is active on Set to 'default' if a non-named candidate is active
Context	system configuration session id number name string
Tree	name
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

started *string*

Description	Start date and time of the configuration session
Context	system configuration session id number started string
Tree	started
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

type *keyword*

Description	Type of configuration session
Context	system configuration session id number type keyword
Tree	type
Options	<ul style="list-style-type: none"> • shared • private
Configurable	False
Platforms	Supported on all platforms

username *string*

Description	User that started the configuration session
Context	system configuration session id number username string
Tree	username
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

dhcp-server

Description	Configures the dhcp server
Context	system dhcp-server
Tree	dhcp-server
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Globally enable or disable the dhcp server Disabling this will disable all dhcp servers.
Context	system dhcp-server admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

network-instance [name](#) *reference*

Description	List of network instances to run a dhcp server in
Context	system dhcp-server network-instance name <i>reference</i>
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	Reference to a configured network instance
Context	system dhcp-server network-instance name <i>reference</i>
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

dhcpv4

Description	Enter the dhcpv4 context
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4
Tree	dhcpv4
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the dhcp server
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details if the dhcp server is operationally available
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

options**Description**

Enter the options context

Context[system dhcp-server network-instance name reference dhcpv4 options](#)**Tree**[options](#)**Configurable**

True

Platforms

Supported on all platforms

bootfile-name *string***Description**

The URL to the provisioning script the client will use during booting

Context[system dhcp-server network-instance name reference dhcpv4 options bootfile-name *string*](#)**Tree**[bootfile-name](#)

String Length	1 to 128
Configurable	True
Platforms	Supported on all platforms

dns-server *string*

Description	An Ordered List of DNS servers to return to the dhcp client
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 options dns-server <i>string</i>
Tree	dns-server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	4

domain-name *string*

Description	The domain name to return to the dhcp client that the client should use when resolving hostnames via the Domain Name System
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 options domain-name <i>string</i>
Tree	domain-name
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

hostname *string*

Description	Host Name option of the dhcp client
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 options hostname <i>string</i>
Tree	hostname
String Length	1 to 63
Configurable	True
Platforms	Supported on all platforms

ntp-server *string*

Description	List of NTP Servers to return to the dhcp client
--------------------	--

Context	system dhcp-server network-instance name reference dhcpv4 options ntp-server string
Tree	ntp-server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	4

router string

Description	IPv4 address of the gateway for the dhcp client
Context	system dhcp-server network-instance name reference dhcpv4 options router string
Tree	router
Configurable	True
Platforms	Supported on all platforms

server-id string

Description	IP address the dhcp server must match any address within the network_instance e.g. sub-interface primary address, loopback address, anycast gateway address in case of multihoming
Context	system dhcp-server network-instance name reference dhcpv4 options server-id string
Tree	server-id
Configurable	True
Platforms	Supported on all platforms

static-allocation

Description	Enter the static-allocation context
Context	system dhcp-server network-instance name reference dhcpv4 static-allocation
Tree	static-allocation
Configurable	True
Platforms	Supported on all platforms

host mac string

Description	host name for static ip allocations
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac string
Tree	host
Configurable	True
Platforms	Supported on all platforms

mac string

Description	Enter the mac context
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac string
Configurable	True
Platforms	Supported on all platforms

ip-address string

Description	Enter the ip-address context
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac string ip-address string
Tree	ip-address
Configurable	True
Platforms	Supported on all platforms

options

Description	Enter the options context
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac string options
Tree	options
Configurable	True
Platforms	Supported on all platforms

bootfile-name string

Description	The URL to the provisioning script the client will use during booting
--------------------	---

Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac <i>string</i> options bootfile-name <i>string</i>
Tree	bootfile-name
String Length	1 to 128
Configurable	True
Platforms	Supported on all platforms

dns-server *string*

Description	An Ordered List of DNS servers to return to the dhcp client
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac <i>string</i> options dns-server <i>string</i>
Tree	dns-server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	4

domain-name *string*

Description	The domain name to return to the dhcp client that the client should use when resolving hostnames via the Domain Name System
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac <i>string</i> options domain-name <i>string</i>
Tree	domain-name
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

hostname *string*

Description	Host Name option of the dhcp client
Context	system dhcp-server network-instance name <i>reference</i> dhcpv4 static-allocation host mac <i>string</i> options hostname <i>string</i>
Tree	hostname
String Length	1 to 63
Configurable	True
Platforms	Supported on all platforms

ntp-server string

Description	List of NTP Servers to return to the dhcp client
Context	system dhcp-server network-instance name reference dhcpv4 static-allocation host mac string options ntp-server string
Tree	ntp-server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	4

router string

Description	IPv4 address of the gateway for the dhcp client
Context	system dhcp-server network-instance name reference dhcpv4 static-allocation host mac string options router string
Tree	router
Configurable	True
Platforms	Supported on all platforms

server-id string

Description	IP address the dhcp server must match any address within the network_instance e.g. sub-interface primary address, loopback address, anycast gateway address in case of multihoming
Context	system dhcp-server network-instance name reference dhcpv4 static-allocation host mac string options server-id string
Tree	server-id
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	system dhcp-server network-instance name reference dhcpv4 statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

client-packets-discarded *number*

Description	Total discarded dhcp packets from dhcp client(s)
Context	system dhcp-server network-instance name reference dhcpv4 statistics client-packets-discarded <i>number</i>
Tree	client-packets-discarded
Default	0
Configurable	False
Platforms	Supported on all platforms

client-packets-received *number*

Description	Total received dhcp packets from dhcp client(s)
Context	system dhcp-server network-instance name reference dhcpv4 statistics client-packets-received <i>number</i>
Tree	client-packets-received
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-sent *number*

Description	Total dhcp packets sent from DHCP server towards dhcp client(s)
Context	system dhcp-server network-instance name reference dhcpv4 statistics server-packets-sent <i>number</i>
Tree	server-packets-sent
Default	0
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Container for tracing DHCP server operations instance
Context	system dhcp-server network-instance name reference dhcpv4 trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace keyword

Description	List of events to trace
Context	system dhcp-server network-instance name reference dhcpv4 trace-options trace keyword
Tree	trace
Options	<ul style="list-style-type: none"> • messages Capture all DHCP server messages sent and received
Configurable	True
Platforms	Supported on all platforms

dhcpv6

Description	Enter the dhcpv6 context
Context	system dhcp-server network-instance name reference dhcpv6
Tree	dhcpv6
Configurable	True
Platforms	Supported on all platforms

admin-state keyword

Description	Administratively enable or disable the dhcp server
Context	system dhcp-server network-instance name reference dhcpv6 admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state keyword

Description	Details if the dhcp server is operationally available
Context	system dhcp-server network-instance name reference dhcpv6 oper-state keyword
Tree	oper-state

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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

options

Description	Enter the options context
Context	system dhcp-server network-instance name <i>reference</i> dhcpv6 options
Tree	options
Configurable	True
Platforms	Supported on all platforms

dns-server *string*

Description	An Ordered List of DNS servers to return to the dhcp client
Context	system dhcp-server network-instance name <i>reference</i> dhcpv6 options dns-server <i>string</i>
Tree	dns-server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	4

static-allocation

Description	Enter the static-allocation context
Context	system dhcp-server network-instance name <i>reference</i> dhcpv6 static-allocation
Tree	static-allocation
Configurable	True
Platforms	Supported on all platforms

host *mac string*

Description	host name for static ip allocations
Context	system dhcp-server network-instance name <i>reference</i> dhcpv6 static-allocation host mac <i>string</i>
Tree	host
Configurable	True
Platforms	Supported on all platforms

mac string

Description	Enter the mac context
Context	system dhcp-server network-instance name reference dhcpv6 static-allocation host mac string
Configurable	True
Platforms	Supported on all platforms

ip-address string

Description	Enter the ip-address context
Context	system dhcp-server network-instance name reference dhcpv6 static-allocation host mac string ip-address string
Tree	ip-address
Configurable	True
Platforms	Supported on all platforms

options

Description	Enter the options context
Context	system dhcp-server network-instance name reference dhcpv6 static-allocation host mac string options
Tree	options
Configurable	True
Platforms	Supported on all platforms

dns-server string

Description	An Ordered List of DNS servers to return to the dhcp client
Context	system dhcp-server network-instance name reference dhcpv6 static-allocation host mac string options dns-server string
Tree	dns-server
Configurable	True
Platforms	Supported on all platforms
Max. Elements	4

statistics

Description	Enter the statistics context
--------------------	------------------------------

Context	system dhcp-server network-instance name reference dhcpv6 statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

client-packets-discarded *number*

Description	Total discarded dhcp packets from dhcp client(s)
Context	system dhcp-server network-instance name reference dhcpv6 statistics client-packets-discarded number
Tree	client-packets-discarded
Default	0
Configurable	False
Platforms	Supported on all platforms

client-packets-received *number*

Description	Total received dhcp packets from dhcp client(s)
Context	system dhcp-server network-instance name reference dhcpv6 statistics client-packets-received number
Tree	client-packets-received
Default	0
Configurable	False
Platforms	Supported on all platforms

server-packets-sent *number*

Description	Total dhcp packets sent from DHCP server towards dhcp client(s)
Context	system dhcp-server network-instance name reference dhcpv6 statistics server-packets-sent number
Tree	server-packets-sent
Default	0
Configurable	False
Platforms	Supported on all platforms

trace-options

Description	Container for tracing DHCP server operations instance
Context	system dhcp-server network-instance name reference dhcpv6 trace-options
Tree	trace-options
Configurable	True
Platforms	Supported on all platforms

trace keyword

Description	List of events to trace
Context	system dhcp-server network-instance name reference dhcpv6 trace-options trace keyword
Tree	trace
Options	<ul style="list-style-type: none"> • messages Capture all DHCP server messages sent and received
Configurable	True
Platforms	Supported on all platforms

dns

Description	Top-level container for DNS configuration and state
Context	system dns
Tree	dns
Configurable	True
Platforms	Supported on all platforms

host-entry [name string](#)

Description	List of static host entries
Context	system dns host-entry name string
Tree	host-entry
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of host entry
Context	system dns host-entry name <i>string</i>
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

ipv4-address *string*

Description	IPv4 address for the host entry
Context	system dns host-entry name <i>string</i> ipv4-address <i>string</i>
Tree	ipv4-address
Configurable	True
Platforms	Supported on all platforms

ipv6-address *string*

Description	IPv6 address for the host entry
Context	system dns host-entry name <i>string</i> ipv6-address <i>string</i>
Tree	ipv6-address
Configurable	True
Platforms	Supported on all platforms

network-instance *reference*

Description	Reference to a configured network-instance to source DNS requests from
Context	system dns network-instance <i>reference</i>
Tree	network-instance
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details the operational state of the DNS client
Context	system dns oper-state <i>keyword</i>

Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

search-list *string*

Description	An ordered list of domains to search when resolving a host name
Context	system dns search-list <i>string</i>
Tree	search-list
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

server-list (*ipv4-address* | *ipv6-address*)

Description	List of the DNS servers that the resolver should query
Context	system dns server-list (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	server-list
Configurable	True
Platforms	Supported on all platforms
Max. Elements	3

features *string*

Description	Features enabled on this platform
Context	system features <i>string</i>
Tree	features
String Length	1 to 255
Configurable	False
Platforms	Supported on all platforms

ftp-server

Description	Top-level container for FTP server configuration and state
Context	system ftp-server
Tree	ftp-server
Configurable	True
Platforms	Supported on all platforms

network-instance *name reference*

Description	List of network-instances to run an FTP server in
Context	system ftp-server network-instance name reference
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	Reference to a configured network-instance
Context	system ftp-server network-instance name reference
Reference	network-instance name string
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enables or disables the FTP server in this network-instance
Context	system ftp-server network-instance name reference admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details the operational state of the FTP server
Context	system ftp-server network-instance name reference oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

session-limit *number***Description**

Set a limit on the number of simultaneous active FTP sessions

Context[system ftp-server network-instance name reference session-limit number](#)**Tree**[session-limit](#)**Default**

20

Configurable	True
Platforms	Supported on all platforms

source-address (*ipv4-address* | *ipv6-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'.
Context	system ftp-server network-instance name reference source-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	source-address
Default	::
Configurable	True
Platforms	Supported on all platforms

timeout *number*

Description	Set the idle timeout in seconds on FTP connections
Context	system ftp-server network-instance name reference timeout <i>number</i>
Tree	timeout
Default	300
Units	seconds
Configurable	True
Platforms	Supported on all platforms

gnmi-server

Description	Configures the gNMI server access API
Context	system gnmi-server
Tree	gnmi-server
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Globally enable or disable the gNMI server. Disabling this will disable all gNMI servers.
Context	system gnmi-server admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

commit-confirmed-timeout *number*

Description	Number of seconds to wait for confirmation. A value of 0 means commit confirmed is not used
Context	system gnmi-server commit-confirmed-timeout number
Tree	commit-confirmed-timeout
Range	0 to 86400
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

commit-save *boolean*

Description	Specifies whether to save startup configuration after every successful commit
Context	system gnmi-server commit-save boolean
Tree	commit-save
Default	false
Configurable	True
Platforms	Supported on all platforms

include-defaults-in-config-only-responses *boolean*

Description	Specifies whether to include field default values in get/subscribe responses when using configuration only datastore (for example running/intended datastore)
Context	system gnmi-server include-defaults-in-config-only-responses <i>boolean</i>
Tree	include-defaults-in-config-only-responses
Default	false
Configurable	True
Platforms	Supported on all platforms

network-instance *name reference*

Description	List of network instances to run a gNMI server in
Context	system gnmi-server network-instance name <i>reference</i>
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	Reference to a configured network instance
Context	system gnmi-server network-instance name <i>reference</i>
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the gNMI server
Context	system gnmi-server network-instance name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details if the gNMI server is operationally available
Context	system gnmi-server network-instance name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that

the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

port *number*

Description	Port the gNMI server will listen on for incoming connections
Context	system gnmi-server network-instance name <i>reference</i> port number
Tree	port
Range	0 to 65535
Default	57400
Configurable	True
Platforms	Supported on all platforms

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

Description	List of IP addresses the gNMI server will listen on within the network instance
Context	system gnmi-server network-instance name <i>reference</i> source-address (ipv4-address ipv6-address)
Tree	source-address
Default	::
Configurable	True
Platforms	Supported on all platforms

tls-profile *reference*

Description	Reference to the TLS profile to use on the gNMI server
Context	system gnmi-server network-instance name <i>reference</i> tls-profile reference
Tree	tls-profile
Reference	system tls server-profile name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every gNMI request
Context	system gnmi-server network-instance name <i>reference</i> use-authentication boolean
Tree	use-authentication
Default	true
Configurable	True
Platforms	Supported on all platforms

yang-models *keyword*

Description	Specify yang-models to be used when origin field is not present in the gnmi requests
Context	system gnmi-server network-instance name <i>reference</i> yang-models keyword
Tree	yang-models
Default	native
Options	<ul style="list-style-type: none"> • native • openconfig
Configurable	True
Platforms	Supported on all platforms

rate-limit *number*

Description	Set a limit on the number of connection attempts per minute
Context	system gnmi-server rate-limit <i>number</i>
Tree	rate-limit
Range	0 to 65535
Default	60
Configurable	True
Platforms	Supported on all platforms

session-limit *number*

Description	Set a limit on the number of simultaneous active gNMI sessions
Context	system gnmi-server session-limit <i>number</i>
Tree	session-limit

Range	0 to 65535
Default	20
Configurable	True
Platforms	Supported on all platforms

subscription *id number*

Description	List of subscriptions
Context	system gnmi-server subscription id number
Tree	subscription
Configurable	False
Platforms	Supported on all platforms

id *number*

Description	System generated ID for for the subscription
Context	system gnmi-server subscription id number
Range	0 to 4294967295
Configurable	False
Platforms	Supported on all platforms

mode *keyword*

Description	Subscription mode (ON_CHANGE, SAMPLE, TARGET_DEFINED, POLL, ONCE)
Context	system gnmi-server subscription id number mode keyword
Tree	mode
Options	<ul style="list-style-type: none"> • ON_CHANGE • SAMPLE • TARGET_DEFINED • POLL • ONCE
Configurable	False
Platforms	Supported on all platforms

paths *string*

Description	List of paths being subscribed to
Context	system gnmi-server subscription id number paths string
Tree	paths
Configurable	False
Platforms	Supported on all platforms

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

Description	Remote host of the subscription
Context	system gnmi-server subscription id number remote-host (ipv4-address ipv6-address)
Tree	remote-host
Configurable	False
Platforms	Supported on all platforms

remote-port *number*

Description	Remote port of the subscription
Context	system gnmi-server subscription id number remote-port number
Tree	remote-port
Range	0 to 65535
Configurable	False
Platforms	Supported on all platforms

sample-interval *number*

Description	Time in seconds to provide updates to the remote host, set to 0 for all subscription modes except SAMPLE
Context	system gnmi-server subscription id number sample-interval number
Tree	sample-interval
Units	seconds
Configurable	False
Platforms	Supported on all platforms

start-time *string*

Description	Time of the subscription creation
Context	system gnmi-server subscription id number start-time string
Tree	start-time
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

user *string*

Description	Authenticated username for the subscription
Context	system gnmi-server subscription id number user string
Tree	user
Configurable	False
Platforms	Supported on all platforms

user-agent *string*

Description	User agent used for the subscription
Context	system gnmi-server subscription id number user-agent string
Tree	user-agent
Configurable	False
Platforms	Supported on all platforms

timeout *number*

Description	Set the idle timeout in seconds on gNMI connections
Context	system gnmi-server timeout number
Tree	timeout
Range	0 to 65535
Default	7200
Units	seconds
Configurable	True
Platforms	Supported on all platforms

trace-options *keyword*

Description	gNMI trace options
Context	system gnmi-server trace-options <i>keyword</i>
Tree	trace-options
Options	<ul style="list-style-type: none"> • request • response • common
Configurable	True
Platforms	Supported on all platforms

unix-socket

Description	Top-level container for configuration and state related to unix sockets
Context	system gnmi-server unix-socket
Tree	unix-socket
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the gNMI server
Context	system gnmi-server unix-socket admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details if the gNMI server is operationally available
Context	system gnmi-server unix-socket oper-state <i>keyword</i>
Tree	oper-state
Options	<ul style="list-style-type: none"> • up <p>Component or process is operational</p>

- 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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

socket-path *string***Description**

Path to the unix socket used by gNMI

Context[system](#) [gnmi-server](#) [unix-socket](#) [socket-path](#) *string*

Tree	socket-path
Configurable	False
Platforms	Supported on all platforms

tls-profile *reference*

Description	Reference to the TLS profile to use on the gNMI unix socket server If none is specified, then TLS is not used.
Context	system gnmi-server unix-socket tls-profile <i>reference</i>
Tree	tls-profile
Reference	system tls server-profile name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every gNMI request
Context	system gnmi-server unix-socket use-authentication <i>boolean</i>
Tree	use-authentication
Default	true
Configurable	True
Platforms	Supported on all platforms

yang-models *keyword*

Description	Specify yang-models to be used when origin field is not present in the gnmi requests
Context	system gnmi-server unix-socket yang-models <i>keyword</i>
Tree	yang-models
Default	native
Options	<ul style="list-style-type: none"> • native • openconfig
Configurable	True
Platforms	Supported on all platforms

gribi-server

Description	Configures the gRPC Routing Information Base Interface (gRIBI) service
Context	system gribi-server
Tree	gribi-server
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description	Globally enable or disable the gRIBI service Disabling this will disable all gRIBI sockets in all configured network-instances (including unix sockets).
Context	system gribi-server admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

client id *number*

Description	List of active gRIBI client sessions
Context	system gribi-server client id <i>number</i>
Tree	client
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

id *number*

Description	System generated ID for for the client
Context	system gribi-server client id <i>number</i>
Range	0 to 4294967295
Configurable	False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

election-id string

Description Election ID of this client

Context [system gribi-server client id number election-id string](#)

Tree [election-id](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

persistence-mode keyword

Description The defined persistence mode as signaled by the client

Context [system gribi-server client id number persistence-mode keyword](#)

Tree [persistence-mode](#)

Options

- preserve
Entries populated by the client will be persisted during a client disconnect, or control module switchover
- delete
Entries populated by the client will be purged on the client disconnecting, or a control module switchover
Entries populated by the client will be purged on the client disconnecting, or a control module switchover If no persistence mode is signaled, the default is to delete entries.

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

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

Description Remote host of the client

Context [system gribi-server client id number remote-host \(ipv4-address | ipv6-address\)](#)

Tree [remote-host](#)

Configurable False

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

remote-port *number*

Description	Remote port of the client
Context	system gribi-server client id number remote-port number
Tree	remote-port
Range	0 to 65535
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

start-time *string*

Description	Time the client first connected
Context	system gribi-server client id number start-time string
Tree	start-time
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

user *string*

Description	Authenticated username for the client
Context	system gribi-server client id number user string
Tree	user
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

user-agent *string*

Description	User agent used for by the client
Context	system gribi-server client id number user-agent string
Tree	user-agent
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

network-instance *name reference*

Description	List of network instances to run a gRIBI socket in
Context	system gribi-server network-instance name reference
Tree	network-instance
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *reference*

Description	Reference to a configured network instance
Context	system gribi-server network-instance name reference
Reference	network-instance name string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description	Administratively enable or disable the gRIBI service
Context	system gribi-server network-instance name reference admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-state *keyword*

Description	Details if the gRIBI service is operationally available
Context	system gribi-server network-instance name reference oper-state keyword
Tree	oper-state
Options	<ul style="list-style-type: none"> • up <p>Component or process is operational</p>

- 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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

port number**Description**

TCP port the gRIBI server will listen on for incoming connections

Context	system gribi-server network-instance name <i>reference</i> port <i>number</i>
Tree	port
Range	0 to 65535
Default	57401
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

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

Description	List of IP addresses the gRIBI server will listen on within the network instance By default the gRIBI server will listen on all addresses in the network-instance.
Context	system gribi-server network-instance name <i>reference</i> source-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	source-address
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

tls-profile *reference*

Description	Reference to the TLS profile to use on the gRIBI server
Context	system gribi-server network-instance name <i>reference</i> tls-profile <i>reference</i>
Tree	tls-profile
Reference	system tls server-profile name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every gRIBI RPC request
Context	system gribi-server network-instance name <i>reference</i> use-authentication <i>boolean</i>
Tree	use-authentication
Default	true

Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

rate-limit number

Description	Set a limit on the number of connection attempts per minute
Context	system gribi-server rate-limit number
Tree	rate-limit
Range	0 to 65535
Default	60
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

session-limit number

Description	Set a limit on the number of simultaneous active gRIBI sessions
Context	system gribi-server session-limit number
Tree	session-limit
Range	0 to 65535
Default	20
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

timeout number

Description	Set the idle timeout in seconds on gRIBI clients
Context	system gribi-server timeout number
Tree	timeout
Range	0 to 65535
Default	7200
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

trace-options *keyword*

Description	gRIBI trace options
Context	system gribi-server trace-options <i>keyword</i>
Tree	trace-options
Options	<ul style="list-style-type: none"> • request • response • common
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

unix-socket

Description	Top-level container for configuration and state related to unix sockets
Context	system gribi-server unix-socket
Tree	unix-socket
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

admin-state *keyword*

Description	Administratively enable or disable the gRIBI service
Context	system gribi-server unix-socket admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-state *keyword*

Description	Details if the gRIBI service is operationally available
Context	system gribi-server unix-socket oper-state <i>keyword</i>

Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

socket-path *string*

Description	Path to the unix socket used by gRIBI
Context	system gribi-server unix-socket socket-path <i>string</i>
Tree	socket-path
Configurable	False
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

tls-profile *reference*

Description	Reference to the TLS profile to use on the gRIBI unix socket server If none is specified, then TLS is not used.
Context	system gribi-server unix-socket tls-profile <i>reference</i>
Tree	tls-profile
Reference	system tls server-profile name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every gRIBI RPC request
Context	system gribi-server unix-socket use-authentication <i>boolean</i>
Tree	use-authentication
Default	true
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

information

Description	Top-level container for system information configuration and state
Context	system information
Tree	information
Configurable	True

Platforms Supported on all platforms

contact *string*

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.

Context [system information contact *string*](#)

Tree [contact](#)

Configurable True

Platforms Supported on all platforms

current-datetime *string*

Description The current system date and time

Context [system information current-datetime *string*](#)

Tree [current-datetime](#)

String Length 20 to 32

Configurable False

Platforms Supported on all platforms

description *string*

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: SR Linux-<version> <hostname> <kernel> <build date>. This field is exposed via SNMP at the sysDescr OID.

Context [system information description *string*](#)

Tree [description](#)

Configurable False

Platforms Supported on all platforms

last-booted *string*

Description The date and time the system was last booted

Context [system information last-booted *string*](#)

Tree	last-booted
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

location string

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.
Context	system information location string
Tree	location
Configurable	True
Platforms	Supported on all platforms

version string

Description	The system version This field represents the version of the management server
Context	system information version string
Tree	version
Configurable	False
Platforms	Supported on all platforms

json-rpc-server

Description	Configures the JSON RPC access API
Context	system json-rpc-server
Tree	json-rpc-server
Configurable	True
Platforms	Supported on all platforms

admin-state keyword

Description	Globally enable or disable the JSON RPC server Disabling this will disable all JSON RPC servers.
--------------------	--

Context	system json-rpc-server admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

commit-confirmed-timeout *number*

Description	Number of seconds to wait for confirmation. A value of 0 means commit confirmed is not used
Context	system json-rpc-server commit-confirmed-timeout <i>number</i>
Tree	commit-confirmed-timeout
Range	0 to 86400
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

network-instance [name](#) *reference*

Description	List of network instances to run the JSON RPC server in
Context	system json-rpc-server network-instance name <i>reference</i>
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	Reference to a configured network-instance
Context	system json-rpc-server network-instance name <i>reference</i>
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

http

Description	Top-level container for the JSON RPC HTTP server
Context	system json-rpc-server network-instance name reference http
Tree	http
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the HTTP JSON RPC server This requires the JSON RPC server to be globally enabled
Context	system json-rpc-server network-instance name reference http admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details if the JSON RPC server is operationally available
Context	system json-rpc-server network-instance name reference http oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

port number**Description**

The port the HTTP JSON RPC server will listen on for incoming connections

Context[system json-rpc-server network-instance name reference http port number](#)**Tree**[port](#)**Range**

0 to 65535

Default

80

Configurable

True

Platforms

Supported on all platforms

session-limit *number*

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.
Context	system json-rpc-server network-instance name <i>reference</i> http session-limit number
Tree	session-limit
Range	1 to 100
Default	10
Configurable	True
Platforms	Supported on all platforms

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

Description	List of IP addresses the JSON RPC server will listen on within the network instance
Context	system json-rpc-server network-instance name <i>reference</i> http source-address (ipv4-address ipv6-address)
Tree	source-address
Default	::
Configurable	True
Platforms	Supported on all platforms

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every JSON RPC request
Context	system json-rpc-server network-instance name <i>reference</i> http use-authentication boolean
Tree	use-authentication
Default	true
Configurable	True
Platforms	Supported on all platforms

https

Description	Top-level container for the JSON-RPC HTTPS server
Context	system json-rpc-server network-instance name <i>reference</i> https

Tree	https
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable the HTTPS JSON RPC server This requires the JSON RPC server to be globally enabled
Context	system json-rpc-server network-instance name <i>reference</i> https admin-state keyword
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details if the JSON RPC server is operationally available
Context	system json-rpc-server network-instance name <i>reference</i> https oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

Supported on all platforms

port number**Description**

Port the HTTPS JSON RPC server will listen on for incoming connections

Context[system json-rpc-server network-instance name reference https port number](#)**Tree**[port](#)**Range**

0 to 65535

Default

443

Configurable

True

Platforms

Supported on all platforms

session-limit number**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.

Context	system json-rpc-server network-instance name reference https session-limit number
Tree	session-limit
Range	1 to 100
Default	10
Configurable	True
Platforms	Supported on all platforms

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

Description	List of IP addresses the JSON RPC server will listen on within the network instance
Context	system json-rpc-server network-instance name reference https source-address (ipv4-address ipv6-address)
Tree	source-address
Default	::
Configurable	True
Platforms	Supported on all platforms

tls-profile *reference*

Description	Reference to the TLS profile to use on the HTTP JSON RPC server
Context	system json-rpc-server network-instance name reference https tls-profile reference
Tree	tls-profile
Reference	system tls server-profile name string
Configurable	True
Platforms	Supported on all platforms

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every JSON RPC request
Context	system json-rpc-server network-instance name reference https use-authentication boolean
Tree	use-authentication
Default	true
Configurable	True

Platforms Supported on all platforms

trace-options *keyword*

Description JSON RPC trace options

Context [system json-rpc-server trace-options](#) *keyword*

Tree [trace-options](#)

Options

- request
- response
- common

Configurable True

Platforms Supported on all platforms

unix-socket

Description Top-level container for configuration and state related to unix sockets

Context [system json-rpc-server unix-socket](#)

Tree [unix-socket](#)

Configurable True

Platforms Supported on all platforms

admin-state *keyword*

Description Administratively enable or disable the JSON RPC server via unix socket This requires the JSON RPC server to be globally enabled

Context [system json-rpc-server unix-socket admin-state](#) *keyword*

Tree [admin-state](#)

Default disable

Options

- enable
- disable

Configurable True

Platforms Supported on all platforms

oper-state *keyword*

Description Details if the JSON RPC server is operationally available

Context	system json-rpc-server unix-socket oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the <code>reinvoke-with-delay</code> action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

socket-path *string*

Description	Path to the unix socket used by JSON RPC
Context	system json-rpc-server unix-socket socket-path <i>string</i>
Tree	socket-path
Configurable	False
Platforms	Supported on all platforms

tls-profile *reference*

Description	Reference to the TLS profile to use on the JSON RPC unix socket server If none is specified, then TLS is not used.
Context	system json-rpc-server unix-socket tls-profile <i>reference</i>
Tree	tls-profile
Reference	system tls server-profile name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

use-authentication *boolean*

Description	Enable or disable the use of username/password authentication for every JSON RPC request
Context	system json-rpc-server unix-socket use-authentication <i>boolean</i>
Tree	use-authentication
Default	true
Configurable	True
Platforms	Supported on all platforms

l2cp-transparency

Description	Enclosing container for system level Layer-2 Control Protocol transparency.
Context	system l2cp-transparency
Tree	l2cp-transparency
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

I2cp-statistics

Description	Container for Layer-2 Control Plane protocol statistics.
Context	system l2cp-transparency l2cp-statistics
Tree	l2cp-statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dot1x

Description	Container for 802.1x protocols.
Context	system l2cp-transparency l2cp-statistics dot1x
Tree	dot1x
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-trap-to-cpu-packets *number*

Description	System level incoming 802.1x frames copied to CPU. Cumulative of all Ethernet interfaces including all the copy-to-cpu 802.1x frames. 802.1x frames are identified by a destination MAC value of 01:80:c2:00:00:03 and EtherType value of 0x888e.
Context	system l2cp-transparency l2cp-statistics dot1x in-trap-to-cpu-packets number
Tree	in-trap-to-cpu-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-tunneled-packets *number*

Description	System level incoming 802.1x tunneled frames. Cumulative of all Ethernet interfaces including all the tunneled 802.1x frames. 802.1x frames are identified by a destination MAC value of 01:80:c2:00:00:03 and EtherType value of 0x888e.
Context	system l2cp-transparency l2cp-statistics dot1x in-tunneled-packets number
Tree	in-tunneled-packets
Default	0
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description Timestamp of the last time the LACP counters were cleared.

Context [system l2cp-transparency l2cp-statistics dot1x last-clear](#) *string*

Tree [last-clear](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lACP

Description Container for LACP.

Context [system l2cp-transparency l2cp-statistics lACP](#)

Tree [lACP](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-trap-to-cpu-packets *number*

Description System level incoming Link Aggregation Control Protocol frames copied to CPU.

Cumulative of all Ethernet interfaces including all the copy-to-cpu LACP frames. LACP frames are identified by a destination MAC value of 01:80:c2:00:00:02, EtherType value of 0x8809 and slow protocol subtype 0x1.

Context [system l2cp-transparency l2cp-statistics lACP in-trap-to-cpu-packets](#) *number*

Tree [in-trap-to-cpu-packets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-tunneled-packets *number*

Description System level incoming Link Aggregation Control Protocol tunneled frames.

Cumulative of all Ethernet interfaces including all the tunneled LACP frames. LACP frames are identified by a destination MAC value of 01:80:c2:00:00:02, EtherType value of 0x8809 and slow protocol subtype 0x1.

Context	system l2cp-transparency l2cp-statistics lacp in-tunneled-packets <i>number</i>
Tree	in-tunneled-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Timestamp of the last time the LACP counters were cleared.
Context	system l2cp-transparency l2cp-statistics lacp last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Timestamp of the last time the L2CP counters were cleared.
Context	system l2cp-transparency l2cp-statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lldp

Description	Container for LLDP.
Context	system l2cp-transparency l2cp-statistics lldp
Tree	lldp
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-trap-to-cpu-packets *number*

Description	System level incoming Link Layer Discovery Protocol frames copied to CPU. Cumulative of all Ethernet interfaces including all the copy-to-cpu LLDP frames. LLDP frames are identified by a destination MAC value of 01:80:c2:00:00:0e and EtherType value of 0x88cc.
Context	system l2cp-transparency l2cp-statistics lldp in-trap-to-cpu-packets number
Tree	in-trap-to-cpu-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-tunneled-packets *number*

Description	System level incoming Link Layer Discovery Protocol tunneled frames. Cumulative of all Ethernet interfaces including all the tunneled LLDP frames. LLDP frames are identified by a destination MAC value of 01:80:c2:00:00:0e and EtherType value of 0x88cc.
Context	system l2cp-transparency l2cp-statistics lldp in-tunneled-packets number
Tree	in-tunneled-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Timestamp of the last time the LACP counters were cleared.
Context	system l2cp-transparency l2cp-statistics lldp last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ptp

Description	Container for Precision Time Protocol Peer-Delay protocol.
Context	system l2cp-transparency l2cp-statistics ptp
Tree	ptp

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-trap-to-cpu-packets *number*

Description	System level incoming Precision Time Protocol Peer-Delay frames copied to CPU. Cumulative of all Ethernet interfaces including all the copy-to-cpu PTP frames. PTP frames are identified by a destination MAC value of 01:80:c2:00:00:0e and Ethertype value of 0x88F7.
Context	system l2cp-transparency l2cp-statistics ptp in-trap-to-cpu-packets <i>number</i>
Tree	in-trap-to-cpu-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-tunneled-packets *number*

Description	System level incoming Precision Time Protocol Peer-Delay tunneled frames. Cumulative of all Ethernet interfaces including all the tunneled PTP frames. PTP frames are identified by a destination MAC value of 01:80:c2:00:00:0e and Ethertype value of 0x88F7.
Context	system l2cp-transparency l2cp-statistics ptp in-tunneled-packets <i>number</i>
Tree	in-tunneled-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Timestamp of the last time the PTP counters were cleared.
Context	system l2cp-transparency l2cp-statistics ptp last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-in-discarded-packets *number*

Description	System level incoming L2CP discarded frames. Cumulative of all Ethernet interfaces including all the discarded L2CP frames. L2CP frames are identified by a destination MAC value of 01:80:c2:00:00:0X or 01:80:c2:00:00:2X, being X any value in the 0..F range.
Context	system l2cp-transparency l2cp-statistics total-in-discarded-packets <i>number</i>
Tree	total-in-discarded-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-in-packets *number*

Description	System level total incoming L2CP frames. Cumulative of all Ethernet interfaces including the tunneled, discarded and copy-to-cpu L2CP frames. L2CP frames are identified by a destination MAC value of 01:80:c2:00:00:0X or 01:80:c2:00:00:2X, being X any value in the 0..F range.
Context	system l2cp-transparency l2cp-statistics total-in-packets <i>number</i>
Tree	total-in-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-in-trap-to-cpu-packets *number*

Description	System level incoming L2CP copy-to-cpu frames. Cumulative of all Ethernet interfaces including all the L2CP frames that are copied to CPU. L2CP frames are identified by a destination MAC value of 01:80:c2:00:00:0X or 01:80:c2:00:00:2X, being X any value in the 0..F range.
Context	system l2cp-transparency l2cp-statistics total-in-trap-to-cpu-packets <i>number</i>
Tree	total-in-trap-to-cpu-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

total-in-tunneled-packets *number*

Description	System level incoming L2CP tunneled frames. Cumulative of all Ethernet interfaces including all the tunneled L2CP frames. L2CP frames are identified by a destination MAC value of 01:80:c2:00:00:0X or 01:80:c2:00:00:2X, being X any value in the 0..F range.
Context	system l2cp-transparency l2cp-statistics total-in-tunneled-packets <i>number</i>
Tree	total-in-tunneled-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

xstp

Description	Container for Spanning Tree Protocols.
Context	system l2cp-transparency l2cp-statistics xstp
Tree	xstp
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-trap-to-cpu-packets *number*

Description	System level incoming Spanning Tree Protocol frames copied to CPU. Cumulative of all Ethernet interfaces including all the copy-to-cpu Spanning Tree frames. Spanning Tree frames are identified by a destination MAC value of 01:80:c2:00:00:00 and LLC value 0x42.
Context	system l2cp-transparency l2cp-statistics xstp in-trap-to-cpu-packets <i>number</i>
Tree	in-trap-to-cpu-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

in-tunneled-packets *number*

Description	System level incoming Spanning Tree tunneled frames. Cumulative of all Ethernet interfaces including all the tunneled Spanning Tree frames. xSTP frames are identified by a destination MAC value of 01:80:c2:00:00:00 and LLC value 0x42.
--------------------	---

Context	system l2cp-transparency l2cp-statistics xstp in-tunneled-packets <i>number</i>
Tree	in-tunneled-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

last-clear *string*

Description	Timestamp of the last time the xSTP counters were cleared.
Context	system l2cp-transparency l2cp-statistics xstp last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lACP

Description	Enter the lACP context
Context	system lACP
Tree	lACP
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

system-id *string*

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
Context	system lACP system-id <i>string</i>
Tree	system-id
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

system-priority *number*

Description	System priority used by the node on this LAG interface. Lower value is higher priority for determining which node is the controlling system.
--------------------	--

Context	system lacp system-priority <i>number</i>
Tree	system-priority
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lldp

Description	Top-level container for LLDP configuration and state data
Context	system lldp
Tree	lldp
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enable or disable LLDP at the system level
Context	system lldp admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

chassis-id *string*

Description	The Chassis ID is a mandatory TLV which identifies the chassis component of the endpoint identifier associated with the transmitting LLDP agent
Context	system lldp chassis-id <i>string</i>
Tree	chassis-id
Configurable	False
Platforms	Supported on all platforms

chassis-id-type *keyword*

Description	The source for the chassis identifier string
--------------------	--

It is an enumerator defined by the LldpChassisIdSubtype object from IEEE 802.1AB MIB.

Context	system lldp chassis-id-type <i>keyword</i>
Tree	chassis-id-type
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 if Name object defined in IETF RFC 2863 • LOCAL Chassis identifier based on a locally defined value
Configurable	False
Platforms	Supported on all platforms

hello-timer *number*

Description	System level hello timer for the LLDP protocol
Context	system lldp hello-timer <i>number</i>
Tree	hello-timer
Default	30
Units	seconds

Configurable	True
Platforms	Supported on all platforms

hold-multiplier *number*

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.
Context	system lldp hold-multiplier number
Tree	hold-multiplier
Default	4
Configurable	True
Platforms	Supported on all platforms

interface [name reference](#)

Description	List of interfaces on which LLDP can be enabled
Context	system lldp interface name reference
Tree	interface
Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	Reference to the LLDP Ethernet interface
Context	system lldp interface name reference
Reference	interface name string
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enable or disable LLDP on the interface
Context	system lldp interface name reference admin-state keyword
Tree	admin-state

Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

neighbor id *string*

Description	List of LLDP neighbors on this interface
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i>
Tree	neighbor
Configurable	False
Platforms	Supported on all platforms

id *string*

Description	System generated identifier for the remote neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i>
Configurable	False
Platforms	Supported on all platforms

capability name *identityref*

Description	List of LLDP system capabilities advertised by the neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> capability name <i>identityref</i>
Tree	capability
Configurable	False
Platforms	Supported on all platforms

name *identityref*

Description	<p>Name of the system capability advertised by the neighbor</p> <p>Capabilities are represented in a bitmap that defines the primary functions of the system. The capabilities are defined in IEEE 802.1AB.</p>
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> capability name <i>identityref</i>

Options	<ul style="list-style-type: none"> • OTHER Other capability not specified; bit position 1 • REPEATER Repeater capability; bit position 2 • MAC_BRIDGE MAC bridge capability; bit position 3 • WLAN_ACCESS_POINT WLAN access point capability; bit position 4 • ROUTER Router; bit position 5 • TELEPHONE Telephone capability; bit position 6 • DOCSIS_CABLE_DEVICE DOCSIS cable device; bit position 7 • STATION_ONLY Station only capability, for devices that implement only an end station capability, and for which none of the other capabilities apply; bit position 8 • C_VLAN C-VLAN component of a VLAN Bridge; bit position 9 • S_VLAN S-VLAN component of a VLAN Bridge; bit position 10 • TWO_PORT_MAC_RELAY Two-port MAC Relay (TPMR) capability; bit position 11
Configurable	False
Platforms	Supported on all platforms

enabled *boolean*

Description	Indicates whether the corresponding system capability is enabled on the neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> capability name <i>identityref</i> enabled <i>boolean</i>
Tree	enabled
Configurable	False
Platforms	Supported on all platforms

chassis-id string

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
Context	system lldp interface name <i>reference</i> neighbor id string chassis-id string
Tree	chassis-id
Configurable	False
Platforms	Supported on all platforms

chassis-id-type keyword

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.
Context	system lldp interface name <i>reference</i> neighbor id string chassis-id-type keyword
Tree	chassis-id-type
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 if Name object defined in IETF RFC 2863

- LOCAL

Chassis identifier based on a locally defined value

Configurable	False
Platforms	Supported on all platforms

custom-tlv *type number oui string oui-subtype string*

Description	List of custom LLDP TLVs from a neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type number <i>string</i> oui <i>string</i> oui-subtype <i>string</i>
Tree	custom-tlv
Configurable	False
Platforms	Supported on all platforms

type *number*

Description	The integer value identifying the type of information contained in the value field.
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type number <i>string</i> oui <i>string</i> oui-subtype <i>string</i>
Configurable	False
Platforms	Supported on all platforms

oui *string*

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].
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type number <i>string</i> oui <i>string</i> oui-subtype <i>string</i>
Configurable	False
Platforms	Supported on all platforms

oui-subtype *string*

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.
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type number oui <i>string</i> oui-subtype <i>string</i>
Configurable	False
Platforms	Supported on all platforms

value *binary*

Description	A variable-length octet-string containing the value for this TLV
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> custom-tlv type number oui <i>string</i> oui-subtype <i>string</i> value <i>binary</i>
Tree	value
Configurable	False
Platforms	Supported on all platforms

first-message *string*

Description	Date and time of the first message from neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> first-message <i>string</i>
Tree	first-message
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

last-update *string*

Description	Date and time of the last update from neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> last-update <i>string</i>
Tree	last-update
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

management-address *address string*

Description	List of management addresses received from the remote LLDP neighbor
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> management-address <i>address string</i>
Tree	management-address
Configurable	False
Platforms	Supported on all platforms

address *string*

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.
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> management-address <i>address string</i>
Configurable	False
Platforms	Supported on all platforms

type *keyword*

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.
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> management-address <i>address string type keyword</i>
Tree	type
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
Platforms	Supported on all platforms

port-description *string*

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.

Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> port-description <i>string</i>
Tree	port-description
Configurable	False
Platforms	Supported on all platforms

port-id (*string* | *binary*)

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.
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> port-id (<i>string</i> <i>binary</i>)
Tree	port-id
Configurable	False
Platforms	Supported on all platforms

port-id-type *keyword*

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.
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> port-id-type <i>keyword</i>
Tree	port-id-type
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 if Name 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
Platforms	Supported on all platforms

system-description *string*

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>
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> system-description <i>string</i>
Tree	system-description
String Length	0 to 255
Configurable	False
Platforms	Supported on all platforms

system-name *string*

Description	<p>The administratively assigned name of the remote neighbor</p> <p>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.</p>
Context	system lldp interface name <i>reference</i> neighbor id <i>string</i> system-name <i>string</i>
Tree	system-name
String Length	0 to 255

Configurable	False
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details the operational state of LLDP on the interface
Context	system lldp interface name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting

Component or process is currently waiting This state can be set by event handler when the `reinvoke-with-delay` action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

statistics

Description	LLDP counters on each interface
Context	system lldp interface name <i>reference</i> statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

frame-discard *number*

Description	The number of LLDP frames received and discarded
Context	system lldp interface name <i>reference</i> statistics frame-discard <i>number</i>
Tree	frame-discard
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-error-in *number*

Description	The number of LLDP frames received with errors
Context	system lldp interface name <i>reference</i> statistics frame-error-in <i>number</i>
Tree	frame-error-in
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-error-out *number*

Description	The number of frame transmit errors on the interface
Context	system lldp interface name <i>reference</i> statistics frame-error-out <i>number</i>

Tree	frame-error-out
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-in *number*

Description	The number of LLDP frames received
Context	system lldp interface name <i>reference</i> statistics frame-in <i>number</i>
Tree	frame-in
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-out *number*

Description	The number of LLDP frames transmitted
Context	system lldp interface name <i>reference</i> statistics frame-out <i>number</i>
Tree	frame-out
Default	0
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Indicates the last time the counters were cleared
Context	system lldp interface name <i>reference</i> statistics last-clear <i>string</i>
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

tlv-discard *number*

Description	The number of TLV frames received and discarded
Context	system lldp interface name <i>reference</i> statistics tlv-discard <i>number</i>

Tree	tlv-discard
Default	0
Configurable	False
Platforms	Supported on all platforms

tlv-unknown *number*

Description	The number of frames received with unknown TLV
Context	system lldp interface name reference statistics tlv-unknown number
Tree	tlv-unknown
Default	0
Configurable	False
Platforms	Supported on all platforms

management-address [subinterface](#) *string*

Description	List of subinterfaces to source management addresses from This list is sent in the management address TLV by LLDP.
Context	system lldp management-address subinterface string
Tree	management-address
Configurable	True
Platforms	Supported on all platforms

subinterface *string*

Description	Reference to the subinterface to source management addresses
Context	system lldp management-address subinterface string
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

type *keyword*

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.
--------------------	--

Context	system lldp management-address subinterface <i>string type keyword</i>
Tree	type
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
Platforms	Supported on all platforms

statistics

Description	Global LLDP counters
Context	system lldp statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

entries-aged-out *number*

Description	The number of entries aged out due to timeout.
Context	system lldp statistics entries-aged-out <i>number</i>
Tree	entries-aged-out
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-discard *number*

Description	The number of LLDP frames received and discarded
Context	system lldp statistics frame-discard <i>number</i>
Tree	frame-discard
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-error-in *number*

Description	The number of LLDP frames received with errors
Context	system lldp statistics frame-error-in number
Tree	frame-error-in
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-in *number*

Description	The number of LLDP frames received
Context	system lldp statistics frame-in number
Tree	frame-in
Default	0
Configurable	False
Platforms	Supported on all platforms

frame-out *number*

Description	The number of LLDP frames transmitted
Context	system lldp statistics frame-out number
Tree	frame-out
Default	0
Configurable	False
Platforms	Supported on all platforms

last-clear *string*

Description	Indicates the last time the counters were cleared
Context	system lldp statistics last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	Supported on all platforms

tlv-accepted *number*

Description	The number of valid TLVs received.
Context	system lldp statistics tlv-accepted number
Tree	tlv-accepted
Default	0
Configurable	False
Platforms	Supported on all platforms

tlv-discard *number*

Description	The number of TLV frames received and discarded
Context	system lldp statistics tlv-discard number
Tree	tlv-discard
Default	0
Configurable	False
Platforms	Supported on all platforms

tlv-unknown *number*

Description	The number of frames received with unknown TLV
Context	system lldp statistics tlv-unknown number
Tree	tlv-unknown
Default	0
Configurable	False
Platforms	Supported on all platforms

system-description *string*

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.
Context	system lldp system-description string
Tree	system-description
String Length	0 to 255
Configurable	False

Platforms Supported on all platforms

system-name *string*

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.

Context [system lldp system-name](#) *string*

Tree [system-name](#)

String Length 0 to 255

Configurable False

Platforms Supported on all platforms

trace-options *keyword*

Description LLDP trace options

Context [system lldp trace-options](#) *keyword*

Tree [trace-options](#)

Options

- received
- transmitted
- common

Configurable True

Platforms Supported on all platforms

load-balancing

Description Adjust system-wide ECMP load balancing options.

Context [system load-balancing](#)

Tree [load-balancing](#)

Configurable True

Platforms Supported on all platforms

hash-options

Description Container for packet header fields and other inputs used in hashing calculations

Context	system load-balancing hash-options
Tree	hash-options
Configurable	True
Platforms	Supported on all platforms

destination-address *boolean*

Description	Include the destination IP address in the hash calculation
Context	system load-balancing hash-options destination-address <i>boolean</i>
Tree	destination-address
Default	true
Configurable	True
Platforms	Supported on all platforms

destination-port *boolean*

Description	Include the destination TCP/UDP port number in the hash calculation if the packet is an unfragmented IP packet carrying a TCP/UDP payload
Context	system load-balancing hash-options destination-port <i>boolean</i>
Tree	destination-port
Default	true
Configurable	True
Platforms	Supported on all platforms

hash-seed *number*

Description	A configured hash seed to override the default value of 0 Different routers can be configured with different hash-seed values to minimize traffic polarization effects. This hash-seed is used by all hash-related CRC calculations including those that take IP header fields, those that take Ethernet header fields and those that take MPLS labels.
Context	system load-balancing hash-options hash-seed <i>number</i>
Tree	hash-seed
Default	0
Configurable	True
Platforms	Supported on all platforms

ipv6-flow-label *boolean*

Description	Include the IPv6 flow label in the hash calculation if the packet is an IPv6 packet It is expected that the IPv6 flow label value is written by the server or other host originating the flow and not changed by any intermediate switch or router.
Context	system load-balancing hash-options ipv6-flow-label <i>boolean</i>
Tree	ipv6-flow-label
Default	false
Configurable	True
Platforms	Supported on all platforms

mpls-label-stack *boolean*

Description	Include the received labels (terminated and non-terminated) in the hash calculation
Context	system load-balancing hash-options mpls-label-stack <i>boolean</i>
Tree	mpls-label-stack
Default	false
Configurable	True
Platforms	Supported on all platforms

protocol *boolean*

Description	Include the IP protocol number in the hash calculation. For an IPv6 packet this is protocol value in the next-header field of the last extension header.
Context	system load-balancing hash-options protocol <i>boolean</i>
Tree	protocol
Default	true
Configurable	True
Platforms	Supported on all platforms

source-address *boolean*

Description	Include the source IP address in the hash calculation
Context	system load-balancing hash-options source-address <i>boolean</i>
Tree	source-address

Default	true
Configurable	True
Platforms	Supported on all platforms

source-port *boolean*

Description	Include the source TCP/UDP port number in the hash calculation if the packet is an unfragmented IP packet carrying a TCP/UDP payload
Context	system load-balancing hash-options source-port <i>boolean</i>
Tree	source-port
Default	true
Configurable	True
Platforms	Supported on all platforms

vlan *boolean*

Description	Include the received VLAN ID in the hash calculation
Context	system load-balancing hash-options vlan <i>boolean</i>
Tree	vlan
Default	true
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

logging

Description	System logging provides the interface to syslog services to setup output entities on a selection of log sources.
Context	system logging
Tree	logging
Configurable	True
Platforms	Supported on all platforms

buffer [buffer-name](#) *string*

Description	Log files maintained in memory, non-persistent across system reboots
--------------------	--

These files are stored at directory `/var/log/srlinux/buffer`. Rotation into multiple files is available.

Context	system logging buffer <code>buffer-name</code> <i>string</i>
Tree	buffer
Configurable	True
Platforms	Supported on all platforms

buffer-name *string*

Description	Base name of the file(s) to be stored in memory
Context	system logging buffer <code>buffer-name</code> <i>string</i>
Configurable	True
Platforms	Supported on all platforms

facility [facility-name](#) *keyword*

Description	List of facilities to source messages from
Context	system logging buffer <code>buffer-name</code> <i>string</i> facility <code>facility-name</code> <i>keyword</i>
Tree	facility
Configurable	True
Platforms	Supported on all platforms

facility-name *keyword*

Description	Name of a Linux syslog facility
Context	system logging buffer <code>buffer-name</code> <i>string</i> facility <code>facility-name</code> <i>keyword</i>
Options	<ul style="list-style-type: none"> • <code>auth</code> • <code>authpriv</code> • <code>cron</code> • <code>daemon</code> • <code>ftp</code> • <code>kern</code> • <code>lpr</code> • <code>mail</code> • <code>news</code> • <code>syslog</code> • <code>user</code>

- uucp
- local0
- local1
- local2
- local3
- local4
- local5
- local6
- local7

Configurable	True
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging buffer buffer-name string facility facility-name keyword priority
Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging buffer buffer-name string facility facility-name keyword priority match-above keyword
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging buffer buffer-name <i>string</i> facility facility-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

filter *reference*

Description	A set of all-matching criteria that messages must fulfill in order to be captured
Context	system logging buffer buffer-name <i>string</i> filter <i>reference</i>
Tree	filter
Reference	system logging filter filter-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

format *string*

Description	Text format of the output syslog messages, in legacy syslog \$template style
Context	system logging buffer buffer-name <i>string</i> format <i>string</i>
Tree	format
Default	%TIMEGENERATED:::date-rfc3339% %HOSTNAME% %SYSLOGTAG% %MSG:::sp-if-no-1st-sp%%MSG:::drop-last-lf%\n
Configurable	True
Platforms	Supported on all platforms

persist *number*

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.
Context	system logging buffer buffer-name <i>string</i> persist <i>number</i>
Tree	persist
Range	0 60 to 604800
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

rotate *number*

Description	Number of files to keep in rotation when a maximum file size is reached
Context	system logging buffer buffer-name <i>string</i> rotate <i>number</i>
Tree	rotate
Default	4
Configurable	True
Platforms	Supported on all platforms

rotations *number*

Description	Number of file rotations occurred
Context	system logging buffer buffer-name <i>string</i> rotations <i>number</i>
Tree	rotations
Default	0
Configurable	False
Platforms	Supported on all platforms

size *string*

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.

Context	system logging buffer buffer-name <i>string size string</i>
Tree	size
Default	10M
Configurable	True
Platforms	Supported on all platforms

subsystem [subsystem-name](#) *keyword*

Description	Entity or entities that may produce messages to be captured
Context	system logging buffer buffer-name <i>string subsystem subsystem-name keyword</i>
Tree	subsystem
Configurable	True
Platforms	Supported on all platforms

subsystem-name *keyword*

Description	Reference to an available subsystem to source messages from
Context	system logging buffer buffer-name <i>string subsystem subsystem-name keyword</i>
Options	<ul style="list-style-type: none"> • aaa • accounting • acl • app • arpd • bfd • bgp • bridgetable • chassis • debug • dhcp • ethcfm • evpn • fib • gnmi

- gribi
- igmp
- isis
- json
- lag
- ldp
- linux
- lldp
- log
- mgmt
- mirror
- mld
- mpls
- netinst
- ospf
- p4rt
- pim
- platform
- policy
- qos
- radio
- sdk
- sflow
- staticroute
- twamp
- vxlan
- xdp

Configurable

True

Platforms

Supported on all platforms

priority

Description

Narrows the capture to a given severity, a range or a specific set of severities

Context

[system logging buffer buffer-name](#) *string* [subsystem subsystem-name](#)
keyword [priority](#)

Tree

[priority](#)

Configurable

True

Platforms Supported on all platforms

match-above *keyword*

Description At a given severity and above

Context [system logging buffer buffer-name](#) *string* [subsystem subsystem-name](#)
keyword [priority match-above](#) *keyword*

Tree [match-above](#)

Options

- emergency
- alert
- critical
- error
- warning
- notice
- informational
- debug

Configurable True

Platforms Supported on all platforms

match-exact *keyword*

Description Individually specified severities

Context [system logging buffer buffer-name](#) *string* [subsystem subsystem-name](#)
keyword [priority match-exact](#) *keyword*

Tree [match-exact](#)

Options

- emergency
- alert
- critical
- error
- warning
- notice
- informational
- debug

Configurable True

Platforms Supported on all platforms

console

Description	Hardware serial device normally used for bring-up and diagnostics
Context	system logging console
Tree	console
Configurable	True
Platforms	Supported on all platforms

facility [facility-name](#) *keyword*

Description	List of facilities to source messages from
Context	system logging console facility facility-name <i>keyword</i>
Tree	facility
Configurable	True
Platforms	Supported on all platforms

facility-name *keyword*

Description	Name of a Linux syslog facility
Context	system logging console facility facility-name <i>keyword</i>
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

	<ul style="list-style-type: none"> • local6 • local7
Configurable	True
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging console facility facility-name keyword priority
Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging console facility facility-name keyword priority match-above keyword
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging console facility facility-name keyword priority match-exact keyword
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency

- alert
- critical
- error
- warning
- notice
- informational
- debug

Configurable	True
Platforms	Supported on all platforms

filter *reference*

Description	A set of all-matching criteria that messages must fulfill in order to be captured
Context	system logging console filter <i>reference</i>
Tree	filter
Reference	system logging filter filter-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

format *string*

Description	Text format of the output syslog messages, in legacy syslog \$template style
Context	system logging console format <i>string</i>
Tree	format
Default	%TIMEGENERATED:::date-utc3339% %HOSTNAME% %SYSLOGTAG% %MSG:::sp-if-no-1st-sp%%MSG:::drop-last-lf%\n
Configurable	True
Platforms	Supported on all platforms

subsystem [subsystem-name](#) *keyword*

Description	Entity or entities that may produce messages to be captured
Context	system logging console subsystem subsystem-name <i>keyword</i>
Tree	subsystem
Configurable	True
Platforms	Supported on all platforms

subsystem-name *keyword*

Description	Reference to an available subsystem to source messages from
Context	system logging console subsystem subsystem-name <i>keyword</i>
Options	<ul style="list-style-type: none">• aaa• accounting• acl• app• arpd• bfd• bgp• bridgetable• chassis• debug• dhcp• ethcfm• evpn• fib• gnmi• gribi• igmp• isis• json• lag• ldp• linux• lldp• log• mgmt• mirror• mld• mpls• netinst• ospf• p4rt• pim• platform

- policy
- qos
- radio
- sdk
- sflow
- staticroute
- twamp
- vxlan
- xdp

Configurable	True
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging console subsystem subsystem-name keyword priority
Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging console subsystem subsystem-name keyword priority match-above keyword
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging console subsystem subsystem-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

file [file-name](#) *string*

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.
Context	system logging file file-name <i>string</i>
Tree	file
Configurable	True
Platforms	Supported on all platforms

file-name *string*

Description	Base name of the file(s) to be stored on disk
Context	system logging file file-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

directory *string*

Description	Fully qualified path of a directory where the log file(s) shall be maintained
--------------------	---

Context	system logging file file-name <i>string</i> directory <i>string</i>
Tree	directory
Default	/var/log/srlinux/file
Configurable	True
Platforms	Supported on all platforms

facility [facility-name](#) *keyword*

Description	List of facilities to source messages from
Context	system logging file file-name <i>string</i> facility facility-name <i>keyword</i>
Tree	facility
Configurable	True
Platforms	Supported on all platforms

facility-name *keyword*

Description	Name of a Linux syslog facility
Context	system logging file file-name <i>string</i> facility facility-name <i>keyword</i>
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

	<ul style="list-style-type: none"> • local7
Configurable	True
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging file file-name <i>string</i> facility facility-name <i>keyword</i> priority
Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging file file-name <i>string</i> facility facility-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging file file-name <i>string</i> facility facility-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency • alert

- critical
- error
- warning
- notice
- informational
- debug

Configurable	True
Platforms	Supported on all platforms

filter *reference*

Description	A set of all-matching criteria that messages must fulfill in order to be captured
Context	system logging file file-name <i>string</i> filter reference
Tree	filter
Reference	system logging filter filter-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

format *string*

Description	Text format of the output syslog messages, in legacy syslog \$template style
Context	system logging file file-name <i>string</i> format string
Tree	format
Default	%TIMEGENERATED:::date-rfc3339% %HOSTNAME% %SYSLOGTAG% %MSG:::sp-if-no-1st-sp%%MSG:::drop-last-lf%\n
Configurable	True
Platforms	Supported on all platforms

rotate *number*

Description	Number of files to keep in rotation when a maximum file size is reached
Context	system logging file file-name <i>string</i> rotate number
Tree	rotate
Default	4
Configurable	True
Platforms	Supported on all platforms

rotations *number*

Description	Number of file rotations occurred
Context	system logging file file-name <i>string rotations number</i>
Tree	rotations
Default	0
Configurable	False
Platforms	Supported on all platforms

size *string*

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.
Context	system logging file file-name <i>string size string</i>
Tree	size
Default	10M
Configurable	True
Platforms	Supported on all platforms

subsystem [subsystem-name](#) *keyword*

Description	Entity or entities that may produce messages to be captured
Context	system logging file file-name <i>string subsystem subsystem-name keyword</i>
Tree	subsystem
Configurable	True
Platforms	Supported on all platforms

subsystem-name *keyword*

Description	Reference to an available subsystem to source messages from
Context	system logging file file-name <i>string subsystem subsystem-name keyword</i>
Options	<ul style="list-style-type: none"> • aaa • accounting • acl • app

-
- arpnd
 - bfd
 - bgp
 - bridgetable
 - chassis
 - debug
 - dhcp
 - ethcfm
 - evpn
 - fib
 - gnmi
 - gribi
 - igmp
 - isis
 - json
 - lag
 - ldp
 - linux
 - lldp
 - log
 - mgmt
 - mirror
 - mld
 - mpls
 - netinst
 - ospf
 - p4rt
 - pim
 - platform
 - policy
 - qos
 - radio
 - sdk
 - sflow
 - staticroute
 - twamp
 - vxlan

	<ul style="list-style-type: none"> • xdp
Configurable	True
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging file file-name <i>string</i> subsystem subsystem-name <i>keyword</i> priority
Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging file file-name <i>string</i> subsystem subsystem-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging file file-name <i>string</i> subsystem subsystem-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency

- alert
- critical
- error
- warning
- notice
- informational
- debug

Configurable	True
Platforms	Supported on all platforms

filter *filter-name string*

Description	Describes a set of criteria that captured messages are required to fulfill
Context	system logging filter filter-name string
Tree	filter
Configurable	True
Platforms	Supported on all platforms

filter-name *string*

Description	Name of the filter
Context	system logging filter filter-name string
Configurable	True
Platforms	Supported on all platforms

contains *string*

Description	Text to find in the MSG property of messages to capture from the stream This is slower than prefix.
Context	system logging filter filter-name string contains string
Tree	contains
Configurable	True
Platforms	Supported on all platforms

facility *facility-name keyword*

Description	List of facilities to source messages from
--------------------	--

Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i>
Tree	facility
Configurable	True
Platforms	Supported on all platforms

facility-name *keyword*

Description	Name of a Linux syslog facility
Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i>
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
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i> priority

Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i> priority match-above <i>keyword</i>
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging filter filter-name <i>string</i> facility facility-name <i>keyword</i> priority match-exact <i>keyword</i>
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

prefix string

Description	Text to be present at the beginning of the MSG property of a message This is a fast lookup.
Context	system logging filter filter-name string prefix string
Tree	prefix
Configurable	True
Platforms	Supported on all platforms

regex string

Description	Extended regular expression to search in the MSG property of messages
Context	system logging filter filter-name string regex string
Tree	regex
Configurable	True
Platforms	Supported on all platforms

tag string

Description	Text to be searched in the SYSLOGTAG property of messages Usually a program name or part of it.
Context	system logging filter filter-name string tag string
Tree	tag
Configurable	True
Platforms	Supported on all platforms

network-instance reference

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.
Context	system logging network-instance reference
Tree	network-instance
Reference	network-instance name string
Configurable	True
Platforms	Supported on all platforms

remote-server host (*ipv4-address* | *ipv6-address* | *domain-name*)

Description	List of output remote syslog servers
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>)
Tree	remote-server
Configurable	True
Platforms	Supported on all platforms

host (*ipv4-address* | *ipv6-address* | *domain-name*)

Description	Domain or IP address of a remote syslog server destination
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>)
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

facility [facility-name](#) *keyword*

Description	List of facilities to source messages from
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) facility facility-name <i>keyword</i>
Tree	facility
Configurable	True
Platforms	Supported on all platforms

facility-name *keyword*

Description	Name of a Linux syslog facility
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) facility facility-name <i>keyword</i>
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
Platforms	Supported on all platforms

priority

Description	Narrows the capture to a given severity, a range or a specific set of severities
Context	system logging remote-server host (ipv4-address ipv6-address domain-name) facility facility-name keyword priority
Tree	priority
Configurable	True
Platforms	Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging remote-server host (ipv4-address ipv6-address domain-name) facility facility-name keyword priority match-above keyword
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning

	<ul style="list-style-type: none"> • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) facility <i>facility-name</i> keyword priority match-exact keyword
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

filter *reference*

Description	A set of all-matching criteria that messages must fulfill in order to be captured
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) filter <i>reference</i>
Tree	filter
Reference	system logging filter filter-name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

remote-port *number*

Description	Transport port for syslog to use for messages sent to a remote server
--------------------	---

Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) remote-port <i>number</i>
Tree	remote-port
Default	514
Configurable	True
Platforms	Supported on all platforms

subsystem [subsystem-name](#) *keyword*

Description	Entity or entities that may produce messages to be captured
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) subsystem subsystem-name <i>keyword</i>
Tree	subsystem
Configurable	True
Platforms	Supported on all platforms

subsystem-name *keyword*

Description	Reference to an available subsystem to source messages from
Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) subsystem subsystem-name <i>keyword</i>
Options	<ul style="list-style-type: none"> • aaa • accounting • acl • app • arpd • bfd • bgp • bridgetable • chassis • debug • dhcp • ethcfm • evpn • fib • gnmi • gribi • igmp

- isis
- json
- lag
- ldp
- linux
- lldp
- log
- mgmt
- mirror
- mld
- mpls
- netinst
- ospf
- p4rt
- pim
- platform
- policy
- qos
- radio
- sdk
- sflow
- staticroute
- twamp
- vxlan
- xdp

Configurable

True

Platforms

Supported on all platforms

priority**Description**

Narrows the capture to a given severity, a range or a specific set of severities

Context[system logging remote-server host](#) ([ipv4-address](#) | [ipv6-address](#) | [domain-name](#)) [subsystem subsystem-name](#) [keyword](#) [priority](#)**Tree**[priority](#)**Configurable**

True

Platforms

Supported on all platforms

match-above *keyword*

Description	At a given severity and above
Context	system logging remote-server host (ipv4-address ipv6-address domain-name) subsystem subsystem-name keyword priority match-above keyword
Tree	match-above
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

match-exact *keyword*

Description	Individually specified severities
Context	system logging remote-server host (ipv4-address ipv6-address domain-name) subsystem subsystem-name keyword priority match-exact keyword
Tree	match-exact
Options	<ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • informational • debug
Configurable	True
Platforms	Supported on all platforms

transport *keyword*

Description	Transport protocol for syslog to use for messages sent to a remote server
--------------------	---

Context	system logging remote-server host (<i>ipv4-address</i> <i>ipv6-address</i> <i>domain-name</i>) transport <i>keyword</i>
Tree	transport
Default	udp
Options	<ul style="list-style-type: none"> • udp • tcp
Configurable	True
Platforms	Supported on all platforms

subsystem-facility *keyword*

Description	Linux facility that internal application subsystems will use
Context	system logging subsystem-facility <i>keyword</i>
Tree	subsystem-facility
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

Platforms Supported on all platforms

maintenance

Description Top-level container for Maintenance Mode configuration

Context [system maintenance](#)

Tree [maintenance](#)

Configurable True

Platforms Supported on all platforms

group name *string*

Description List of user-configured maintenance groups

Context [system maintenance group name *string*](#)

Tree [group](#)

Configurable True

Platforms Supported on all platforms

name *string*

Description Name of the maintenance group.

Context [system maintenance group name *string*](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

maintenance-mode

Description Container with options for activating and deactivating maintenance mode for this group

Context [system maintenance group name *string* maintenance-mode](#)

Tree [maintenance-mode](#)

Configurable True

Platforms Supported on all platforms

admin-state *keyword*

Description	Enable or disable maintenance mode for this group The enable setting is blocked if there is another maintenance group with at least one BGP session in its scope that overlaps with this maintenance group and that other maintenance group is currently in maintenance mode. While a maintenance group is in maintenance mode it is not possible to modify the BGP configuration of its members.
Context	system maintenance group name <i>string</i> maintenance-mode admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

maintenance-profile *reference*

Description	Leaf reference to /system/maintenance/profile/name
Context	system maintenance group name <i>string</i> maintenance-profile <i>reference</i>
Tree	maintenance-profile
Reference	system maintenance profile name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

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.
Context	system maintenance group name <i>string</i> members
Tree	members
Configurable	True
Platforms	Supported on all platforms

bgp

Description	Container for specifying the BGP members of the maintenance group
--------------------	---

Context	system maintenance group name <i>string</i> members bgp
Tree	bgp
Configurable	True
Platforms	Supported on all platforms

network-instance [name](#) *reference*

Description	List of network instances with one or more peers to be placed in maintenance mode
Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i>
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	A unique name identifying the network instance
Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i>
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

neighbor *reference*

Description	<p>List of BGP neighbors that belong to the network instance and that should be part of the maintenance group</p> <p>It is not necessary to list neighbors that are members of peer-groups that are already listed.</p> <p>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.</p>
Context	system maintenance group name <i>string</i> members bgp network-instance name <i>reference</i> neighbor <i>reference</i>
Tree	neighbor
Reference	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address</i> <i>ipv6-address-with-zone</i>)
Configurable	True

Platforms Supported on all platforms

peer-group *reference*

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.

Context [system maintenance group name](#) *string* [members bgp network-instance name](#) *reference* [peer-group](#) *reference*

Tree [peer-group](#)

Reference [network-instance name](#) *string* [protocols bgp group group-name](#) *string*

Configurable True

Platforms Supported on all platforms

isis

Description Container for specifying the ISIS members of the maintenance group

Context [system maintenance group name](#) *string* [members isis](#)

Tree [isis](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

network-instances *reference*

Description List of network instances that should be part of the maintenance group.

Context [system maintenance group name](#) *string* [members isis network-instances](#) *reference*

Tree [network-instances](#)

Reference [network-instance name](#) *string*

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

profile [name](#) *string*

Description Enter the profile list instance

Context	system maintenance profile name <i>string</i>
Tree	profile
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of the maintenance profile
Context	system maintenance profile name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

bgp

Description	Container for BGP policies used to achieve traffic draining
Context	system maintenance profile name <i>string</i> bgp
Tree	bgp
Configurable	True
Platforms	Supported on all platforms

export-policy *reference*

Description	A reference to the pre-configured routing policy to apply as an additional/final export policy on BGP sessions in the maintenance group
Context	system maintenance profile name <i>string</i> bgp export-policy <i>reference</i>
Tree	export-policy
Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

import-policy *reference*

Description	A reference to the pre-configured routing policy to apply as an additional/final import policy on BGP sessions in the maintenance group
Context	system maintenance profile name <i>string</i> bgp import-policy <i>reference</i>
Tree	import-policy

Reference	routing-policy policy name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

isis

Description	Container for ISIS configurations.
Context	system maintenance profile name <i>string</i> isis
Tree	isis
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

overload

Description	Container for ISIS overload configurations.
Context	system maintenance profile name <i>string</i> isis overload
Tree	overload
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

max-metric *boolean*

Description	When set to true transit links are advertised with a wide metric of 0xfffffe and a narrow metric of 0x3f
Context	system maintenance profile name <i>string</i> isis overload max-metric <i>boolean</i>
Tree	max-metric
Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

set-bit *boolean*

Description	When set to true, the Overload bit is set
Context	system maintenance profile name <i>string</i> isis overload set-bit <i>boolean</i>
Tree	set-bit

Default	false
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

management

Description	Enclosing container for options relating to management server
Context	system management
Tree	management
Configurable	True
Platforms	Supported on all platforms

openconfig

Description	Top-level container for options relating to OpenConfig
Context	system management openconfig
Tree	openconfig
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enable or disable the OpenConfig management server This will disable OpenConfig throughout the system, and bring any gRPC servers that use it operationally down.
Context	system management openconfig admin-state keyword
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Indicates the operational state of the OpenConfig management server
Context	system management openconfig oper-state keyword

Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state • warm-reboot Component or process is currently warm rebooting Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes. • waiting Component or process is currently waiting Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
Configurable	False
Platforms	Supported on all platforms

mirroring

Description	Top level container for configuration and operational state for mirroring
Context	system mirroring
Tree	mirroring
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mirroring-instance [name string](#)

Description	Mirroring instances configured on the local system
Context	system mirroring mirroring-instance name string
Tree	mirroring-instance
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	4

name [string](#)

Description	A unique name identifying the mirroring instance
Context	system mirroring mirroring-instance name string
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

admin-state [keyword](#)

Description	This leaf contains the configured, desired state of the mirroring instance.
Context	system mirroring mirroring-instance name string admin-state keyword
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

description *string*

Description	A user-entered description of this mirroring instance.
Context	system mirroring mirroring-instance name <i>string</i> description <i>string</i>
Tree	description
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mirror-destination

Description	Configure mirror destination
Context	system mirroring mirroring-instance name <i>string</i> mirror-destination
Tree	mirror-destination
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

local *string*

Description	subinterface of type local-mirror-dest used as local mirror destination
Context	system mirroring mirroring-instance name <i>string</i> mirror-destination local <i>string</i>
Tree	local
String Length	5 to 25
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

remote

Description	Enable the remote context
Context	system mirroring mirroring-instance name <i>string</i> mirror-destination remote
Tree	remote
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

encap *keyword*

Description	Enter the encap context
--------------------	-------------------------

Context	system mirroring mirroring-instance name <i>string</i> mirror-destination remote encap <i>keyword</i>
Tree	encap
Options	<ul style="list-style-type: none"> l2ogre
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

network-instance *reference*

Description	network instance to initiate remote mirror tunnel
Context	system mirroring mirroring-instance name <i>string</i> mirror-destination remote network-instance <i>reference</i>
Tree	network-instance
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

tunnel-end-points

Description	Enter the tunnel-end-points context
Context	system mirroring mirroring-instance name <i>string</i> mirror-destination remote tunnel-end-points
Tree	tunnel-end-points
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

admin-state *keyword*

Description	This leaf contains the configured, desired state of the remote mirror tunnel
Context	system mirroring mirroring-instance name <i>string</i> mirror-destination remote tunnel-end-points admin-state <i>keyword</i>
Tree	admin-state
Default	enable
Options	<ul style="list-style-type: none"> enable disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dst-ipv4 string

Description	remote mirror tunnel destination endpoint IPv4 address
Context	system mirroring mirroring-instance name string mirror-destination remote tunnel-end-points dst-ipv4 string
Tree	dst-ipv4
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

dst-ipv6 string

Description	remote mirror tunnel destination endpoint IPv6 address
Context	system mirroring mirroring-instance name string mirror-destination remote tunnel-end-points dst-ipv6 string
Tree	dst-ipv6
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

oper-state keyword

Description	This leaf contains the operational state of the remote mirror tunnel
Context	system mirroring mirroring-instance name string mirror-destination remote tunnel-end-points oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

src-ipv4 string**Description**

remote mirror tunnel source endpoint IPv4 address

Context[system mirroring mirroring-instance name string mirror-destination remote tunnel-end-points src-ipv4 string](#)**Tree**[src-ipv4](#)**Configurable**

True

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

src-ipv6 string**Description**

remote mirror tunnel source endpoint IPv6 address

Context[system mirroring mirroring-instance name string mirror-destination remote tunnel-end-points src-ipv6 string](#)**Tree**[src-ipv6](#)

Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

mirror-source

Description	Configure mirror source(s)
Context	system mirroring mirroring-instance name <i>string</i> mirror-source
Tree	mirror-source
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

acl

Description	Enter the acl context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl
Tree	acl
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ipv4-filter *name reference*

Description	Enter the ipv4-filter list instance
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv4-filter <i>name reference</i>
Tree	ipv4-filter
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

name reference

Description	Enter the name context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv4-filter <i>name reference</i>
Reference	acl ipv4-filter <i>name</i> <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

entry *sequence-id reference*

Description	Add a list entry for entry
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv4-filter name <i>reference</i> entry sequence-id <i>reference</i>
Tree	entry
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

sequence-id *reference*

Description	Enter the sequence-id context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv4-filter name <i>reference</i> entry sequence-id <i>reference</i>
Reference	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ipv6-filter *name reference*

Description	Enter the ipv6-filter list instance
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv6-filter name <i>reference</i>
Tree	ipv6-filter
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

name *reference*

Description	Enter the name context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv6-filter name <i>reference</i>
Reference	acl ipv6-filter name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

entry *sequence-id reference*

Description	Add a list entry for entry
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv6-filter name <i>reference</i> entry sequence-id <i>reference</i>
Tree	entry
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

sequence-id *reference*

Description	Enter the sequence-id context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source acl ipv6-filter name <i>reference</i> entry sequence-id <i>reference</i>
Reference	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

interface *name string*

Description	List of interfaces used as mirror source
Context	system mirroring mirroring-instance name <i>string</i> mirror-source interface name <i>string</i>
Tree	interface
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	128

name *string*

Description	Enter the name context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source interface name <i>string</i>
String Length	3 to 20
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

direction *keyword*

Description	The direction of traffic to be mirrored
Context	system mirroring mirroring-instance name <i>string</i> mirror-source interface name <i>string</i> direction <i>keyword</i>
Tree	direction
Default	egress-only
Options	<ul style="list-style-type: none"> • ingress-only • egress-only • ingress-egress
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

subinterface [name](#) *string*

Description	List of subinterfaces used as mirror source
Context	system mirroring mirroring-instance name <i>string</i> mirror-source subinterface name <i>string</i>
Tree	subinterface
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	128

name *string*

Description	Enter the name context
Context	system mirroring mirroring-instance name <i>string</i> mirror-source subinterface name <i>string</i>
String Length	5 to 25
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

direction *keyword*

Description	The direction of traffic to be mirrored
Context	system mirroring mirroring-instance name <i>string</i> mirror-source subinterface name <i>string</i> direction <i>keyword</i>
Tree	direction

Default	egress-only
Options	<ul style="list-style-type: none"> • ingress-only • egress-only • ingress-egress
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-down-reason *keyword*

Description	The reason for the mirroring instance being operational down
Context	system mirroring mirroring-instance name <i>string oper-down-reason keyword</i>
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • mirror-inst-admin-down • no-mirror-source • local-mirror-subif-down • remote-mirror-dst-unreachable
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-state *keyword*

Description	This leaf contains the operational state of the mirroring instance.
Context	system mirroring mirroring-instance name <i>string oper-state keyword</i>
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mtu**Description**

Top-level container for configuration and state data related to the system MTU

Context[system mtu](#)**Tree**[mtu](#)**Configurable**

True

Platforms

Supported on all platforms

default-ip-mtu *number***Description**

System default IP MTU in bytes including the IP header but excluding Ethernet overhead

The 7220 IXR-D1, 7220 IXR-D2, 7220 IXR-D3, 7220 IXR-H2, and 7220 IXR-H3 systems support a maximum IP MTU of 9398 bytes.

Context	system mtu default-ip-mtu number
Tree	default-ip-mtu
Range	1280 to 9486
Default	1500
Configurable	True
Platforms	Supported on all platforms

default-l2-mtu *number*

Description	System default Layer-2 MTU in bytes including ethernet overhead and VLAN tags but excluding 4-bytes FCS The 7220 IXR-D1, 7220 IXR-D2, 7220 IXR-D3, 7220 IXR-H2, and 7220 IXR-H3 systems support a maximum L2 MTU of 9412 bytes.
Context	system mtu default-l2-mtu number
Tree	default-l2-mtu
Range	1500 to 9500
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

default-mpls-mtu *number*

Description	System default MPLS MTU in bytes including the size of the transmitted label stack.
Context	system mtu default-mpls-mtu number
Tree	default-mpls-mtu
Range	1284 to 9496
Default	1508
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

default-port-mtu *number*

Description	System default port MTU in bytes including ethernet overhead but excluding 4-bytes FCS The 7220 IXR-D1, 7220 IXR-D2, 7220 IXR-D3, 7220 IXR-H2, and 7220 IXR-H3 systems support a maximum port MTU of 9412 bytes.
--------------------	---

Context	system mtu default-port-mtu <i>number</i>
Tree	default-port-mtu
Range	1500 to 9500
Configurable	True
Platforms	Supported on all platforms

min-path-mtu *number*

Description	Sets the minimum path MTU to use when receiving an ICMP fragmentation needed message This is controlled via the kernel <code>min_pmtu</code> 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.
Context	system mtu min-path-mtu <i>number</i>
Tree	min-path-mtu
Range	552 to 9232
Default	552
Configurable	True
Platforms	Supported on all platforms

name

Description	Contains configuration and state related to system naming
Context	system name
Tree	name
Configurable	True
Platforms	Supported on all platforms

domain-name *string*

Description	The system domain name
Context	system name domain-name <i>string</i>
Tree	domain-name
String Length	1 to 253
Configurable	True
Platforms	Supported on all platforms

host-name *string*

Description	The system host name
Context	system name host-name <i>string</i>
Tree	host-name
String Length	1 to 63
Configurable	True
Platforms	Supported on all platforms

network-instance

Description	Enable the network-instance context
Context	system network-instance
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

protocols

Description	The routing protocols that are enabled for this network-instance.
Context	system network-instance protocols
Tree	protocols
Configurable	True
Platforms	Supported on all platforms

bgp-vpn

Description	Enable the bgp-vpn context
Context	system network-instance protocols bgp-vpn
Tree	bgp-vpn
Configurable	True
Platforms	Supported on all platforms

bgp-instance *id number*

Description	List of bgp-vpn instances configured in the system network-instance. Only one instance allowed in the current release.
--------------------	--

Context	system network-instance protocols bgp-vpn bgp-instance id number
Tree	bgp-instance
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

id number

Description	The index of the bgp-vpn instance
Context	system network-instance protocols bgp-vpn bgp-instance id number
Range	1 to 2
Configurable	True
Platforms	Supported on all platforms

oper-down-reason keyword

Description	Reason for the system bgp-instance being down
Context	system network-instance protocols bgp-vpn bgp-instance id number oper-down-reason keyword
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • no-loopback-address • no-esi • none • network-instance-oper-down
Configurable	False
Platforms	Supported on all platforms

route-distinguisher

Description	Route Distinguisher (RD) of the bgp-vpn instance.
Context	system network-instance protocols bgp-vpn bgp-instance id number route-distinguisher
Tree	route-distinguisher
Configurable	True
Platforms	Supported on all platforms

rd (*string | string | string | string*)

Description	Route Distinguisher (RD) of the system bgp-vpn instance. The RD is auto-derived as <ip-address>:0 where 'ip-address' is the ipv4 address associated to the subinterface lo0.1.
Context	system network-instance protocols bgp-vpn bgp-instance id number route-distinguisher rd (<i>string string string string</i>)
Tree	rd
Configurable	False
Platforms	Supported on all platforms

route-distinguisher-origin *keyword*

Description	Origin of the operational Route Distinguisher (RD) of the bgp-vpn instance. 'Auto-derived-from-system-ip:0' refers to the RD for the EVPN Ethernet Segment routes that is automatically allocated with the format <ip-address>:0 where 'ip-address' is the ipv4 address associated to the subinterface lo0.1.
Context	system network-instance protocols bgp-vpn bgp-instance id number route-distinguisher route-distinguisher-origin keyword
Tree	route-distinguisher-origin
Options	<ul style="list-style-type: none"> • auto-derived-from-system-ip:0 • none
Configurable	False
Platforms	Supported on all platforms

route-target

Description	Route Target (RT) of the system bgp-vpn instance.
Context	system network-instance protocols bgp-vpn bgp-instance id number route-target
Tree	route-target
Configurable	True
Platforms	Supported on all platforms

export-route-target-origin *keyword*

Description	Origin of the operational export Route Target (RT) of the bgp-vpn instance.
--------------------	---

'Auto-derived-from-esi-bytes-1-6' refers to the ES-import RT for the EVPN Ethernet Segment routes that is derived from bytes 1 to 6 of the Ethernet Segment Identifier of the route.

Context	system network-instance protocols bgp-vpn bgp-instance id number route-target export-route-target-origin keyword
Tree	export-route-target-origin
Options	<ul style="list-style-type: none"> • auto-derived-from-esi-bytes-1-6 • none
Configurable	False
Platforms	Supported on all platforms

export-rt (*string* | *string* | *string*)

Description	<p>Export Route Target (RT) in the system bgp-vpn instance.</p> <p>When used for evpn ES routes as ES-import Route Target, the RT is auto-derived from the high-order 6-octet portion of the 9-octet ESI value. Note that the ESI value excludes the left-most byte, which is reserved for the ESI type. The RT is encoded into the ES-import extended community advertised along with the ES route.</p>
Context	system network-instance protocols bgp-vpn bgp-instance id number route-target export-rt (<i>string</i> <i>string</i>)
Tree	export-rt
Configurable	False
Platforms	Supported on all platforms

import-route-target-origin *keyword*

Description	<p>Origin of the operational import Route Target (RT) of the bgp-vpn instance.</p> <p>'Auto-derived-from-esi-bytes-1-6' refers to the ES-import RT for the EVPN Ethernet Segment routes that is derived from bytes 1 to 6 of the Ethernet Segment Identifier of the route.</p>
Context	system network-instance protocols bgp-vpn bgp-instance id number route-target import-route-target-origin keyword
Tree	import-route-target-origin
Options	<ul style="list-style-type: none"> • auto-derived-from-esi-bytes-1-6 • none
Configurable	False
Platforms	Supported on all platforms

import-rt (*string* | *string* | *string*)

Description	Import Route Target (RT) in the system bgp-vpn instance. When used for evpn ES routes as ES-import Route Target, the RT is auto-derived from the high-order 6-octet portion of the 9-octet ESI value. Note that the ESI value excludes the left-most byte, which is reserved for the ESI type. The RT is encoded into the ES-import extended community received along with the ES route.
Context	system network-instance protocols bgp-vpn bgp-instance id number route-target import-rt (<i>string</i> <i>string</i>)
Tree	import-rt
Configurable	False
Platforms	Supported on all platforms

evpn

Description	Enable the evpn context
Context	system network-instance protocols evpn
Tree	evpn
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ethernet-segments

Description	Enable the ethernet-segments context
Context	system network-instance protocols evpn ethernet-segments
Tree	ethernet-segments
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bgp-instance id *reference*

Description	bgp global instances configured in net-instance
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference
Tree	bgp-instance
Configurable	True

Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	1

id *reference*

Description	Enter the id context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference
Reference	system network-instance protocols bgp-vpn bgp-instance id number
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ethernet-segment *name string*

Description	Ethernet Segment configuration and state.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string
Tree	ethernet-segment
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	128

name *string*

Description	A unique name identifying the ethernet segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string
String Length	1 to 32
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

admin-state *keyword*

Description	Admin state of the ethernet segment
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string admin-state keyword
Tree	admin-state
Default	disable

Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

association

Description	Enter the association context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association
Tree	association
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

network-instance [name string](#)

Description	network instance associated to this ethernet-segment
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string
Tree	network-instance
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

name [string](#)

Description	Enter the name context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bgp-instance [instance number](#)

Description	bgp-instance associated to this ethernet-segment
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number

Tree	bgp-instance
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

instance *number*

Description	Enter the instance context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

computed-designated-forwarder-candidates

Description	Enter the computed-designated-forwarder-candidates context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number computed-designated-forwarder-candidates
Tree	computed-designated-forwarder-candidates
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

designated-forwarder-candidate [address \(ipv4-address | ipv6-address\)](#)

Description	designated forwarder candidates for this evi
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number computed-designated-forwarder-candidates designated-forwarder-candidate address (ipv4-address ipv6-address)
Tree	designated-forwarder-candidate
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

address [\(ipv4-address | ipv6-address\)](#)

Description	Enter the address context
--------------------	---------------------------

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number computed-designated-forwarder-candidates designated-forwarder-candidate address \(ipv4-address | ipv6-address\)](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

add-time string

Description The date and time when the designated-forwarder-candidate was added to the designated forwarder candidate list for this evi

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number computed-designated-forwarder-candidates designated-forwarder-candidate address \(ipv4-address | ipv6-address\) add-time string](#)

Tree [add-time](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

designated-forwarder boolean

Description Indicates if this designated-forwarder-candidate is the designated-forwarder.

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number computed-designated-forwarder-candidates designated-forwarder-candidate address \(ipv4-address | ipv6-address\) designated-forwarder boolean](#)

Tree [designated-forwarder](#)

Default false

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

designated-forwarder-activation-start-time string

Description Indicates the time at which the designated-forwarder activation timer started.

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number designated-forwarder-activation-start-time string](#)

Tree	designated-forwarder-activation-start-time
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

designated-forwarder-activation-time *number*

Description	Indicates the number of seconds for the activation timer to run, for this node to become the designated forwarder for this bgp instance.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number designated-forwarder-activation-time number
Tree	designated-forwarder-activation-time
Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

designated-forwarder-role-last-change *string*

Description	Indicates the time at which the designated-forwarder role was changed.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string association network-instance name string bgp-instance instance number designated-forwarder-role-last-change string
Tree	designated-forwarder-role-last-change
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

autodiscovery-per-ethernet-segment-routes

Description	Enter the autodiscovery-per-ethernet-segment-routes context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes
Tree	autodiscovery-per-ethernet-segment-routes
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes attr-id reference
Tree	attr-id
Reference	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

esi string

Description	The Ethernet Segment Identifier encoded in the NLRI
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes esi string
Tree	esi
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ethernet-tag-id number

Description	The 32-bit Ethernet Tag ID encoded in the NLRI. The Ethernet Tag ID identifies a broadcast domain.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes ethernet-tag-id number
Tree	ethernet-tag-id
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

neighbor (ipv4-address | ipv6-address)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes neighbor (ipv4-address ipv6-address)

Tree	neighbor
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

route-distinguisher (*string* | *string* | *string* | *string*)

Description	The route distinguisher encoded in the NLRI.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes route-distinguisher (string string string string)
Tree	route-distinguisher
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vni number

Description	The VXLAN Network Identifier
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string autodiscovery-per-ethernet-segment-routes vni number
Tree	vni
Range	0 to 16777215
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

df-election

Description	Enter the df-election context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election
Tree	df-election
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

algorithm

Description	Enter the algorithm context
--------------------	-----------------------------

Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm
Tree	algorithm
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

manual-alg

Description	Enable the manual-alg context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm manual-alg
Tree	manual-alg
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

primary-evi-range [start-evi number](#)

Description	evi range for this ethernet-segment
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm manual-alg primary-evi-range start-evi number
Tree	primary-evi-range
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

start-evi [number](#)

Description	start of the evi-range for this ethernet-segment
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm manual-alg primary-evi-range start-evi number
Range	1 to 65535
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

end-evi [number](#)

Description	end of the evi-range for this ethernet-segment
--------------------	--

Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm manual-alg primary-evi-range start-evi number end-evi number
Tree	end-evi
Range	1 to 65535
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-type *keyword*

Description	Operational Designated Forwarder algorithm type for this ethernet-segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm oper-type keyword
Tree	oper-type
Options	<ul style="list-style-type: none"> • default • preference • manual
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

preference-alg

Description	Enable the preference-alg context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg
Tree	preference-alg
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

capabilities

Description	Enter the capabilities context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg capabilities
Tree	capabilities
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ac-df *keyword*

Description Attachment Circuit influenced DF Election.

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg capabilities ac-df keyword](#)

Tree [ac-df](#)

Default include

Options

- include
- exclude

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

non-revertive *boolean*

Description Non Revertive mode. If set to true, the 'Don't Preempt Me' capability is advertised in the ES route.

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg capabilities non-revertive boolean](#)

Tree [non-revertive](#)

Default false

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-do-not-preempt *boolean*

Description Operational do-not-preempt value

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg oper-do-not-preempt boolean](#)

Tree [oper-do-not-preempt](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-preference-value *number*

Description	Operational Preference value
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg oper-preference-value number
Tree	oper-preference-value
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

preference-value *number*

Description	Preference that is used to elect the designated forwarder
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm preference-alg preference-value number
Tree	preference-value
Range	0 to 65535
Default	32767
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *keyword*

Description	Designated Forwarder algorithm type for this ethernet-segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string df-election algorithm type keyword
Tree	type
Default	default
Options	<ul style="list-style-type: none"> • default • preference • manual
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

interface-standby-signaling-on-non-df

Description	Enable the interface-standby-signaling-on-non-df context
--------------------	--

Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference</i> ethernet-segment name <i>string</i> df-election interface-standby-signaling-on-non-df
Tree	interface-standby-signaling-on-non-df
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

timers

Description	Enter the timers context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference</i> ethernet-segment name <i>string</i> df-election timers
Tree	timers
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

activation-timer *number*

Description	Remaining activation timer per Ethernet segment
Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference</i> ethernet-segment name <i>string</i> df-election timers activation-timer <i>number</i>
Tree	activation-timer
Range	0 to 100
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

esi *string*

Description	The 10-byte Ethernet Segment Identifier of the ethernet segment. ESI-0 or MAX-ESI values are not allowed. ESI values with bytes 1-6 all zeros are not allowed since they would produce a null ESI-import route-target.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference</i> ethernet-segment name <i>string</i> esi <i>string</i>
Tree	esi
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ethernet-segment-routes

Description	Enter the ethernet-segment-routes context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string ethernet-segment-routes
Tree	ethernet-segment-routes
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

attr-id reference

Description	Leaf reference to networkinstance/protocols/bgp/rib/attr-sets/attr-set/index.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string ethernet-segment-routes attr-id reference
Tree	attr-id
Reference	network-instance name string bgp-rib attr-sets attr-set attr-set-type keyword index number
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

esi string

Description	The Ethernet Segment Identifier
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string ethernet-segment-routes esi string
Tree	esi
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

neighbor (ipv4-address | ipv6-address)

Description	If the route was learned from a BGP neighbor, this is the IPv4 or IPv6 address of that neighbor.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string ethernet-segment-routes neighbor (ipv4-address ipv6-address)
Tree	neighbor
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

originating-router (*ipv4-address* | *ipv6-address*)

Description The IPv4 or IPv6 address of the originating router

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string ethernet-segment-routes originating-router \(ipv4-address | ipv6-address\)](#)

Tree [originating-router](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

route-distinguisher (*string* | *string* | *string* | *string*)

Description The route distinguisher encoded in the NLRI.

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string ethernet-segment-routes route-distinguisher \(string | string | string | string\)](#)

Tree [route-distinguisher](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

interface [ethernet-interface reference](#)

Description Add a list entry for interface

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string interface ethernet-interface reference](#)

Tree [interface](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

Max. Elements 1

ethernet-interface *reference*

Description Interface associated with the ethernet segment.

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string interface ethernet-interface reference](#)

Reference	interface name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

multi-homing-mode *keyword*

Description	Multi-homing mode of the ethernet segment. The state of this leaf can be different than the configured value in cases where the configured value is 'all-active' and the multi-homing mode advertised by the ES peers in the AD per-ES routes is 'single-active'. In this case, the state of this leaf will show 'single-active'.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference ethernet-segment name string multi-homing-mode keyword</i>
Tree	multi-homing-mode
Default	all-active
Options	<ul style="list-style-type: none"> • all-active • single-active
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

next-hop [l3-next-hop](#) (*ipv4-address* | *ipv6-address*)

Description	Enter the next-hop list instance
Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference ethernet-segment name string next-hop l3-next-hop (ipv4-address ipv6-address)</i>
Tree	next-hop
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	1

[l3-next-hop](#) (*ipv4-address* | *ipv6-address*)

Description	Layer-3 next-hop associated with the ethernet segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id <i>reference ethernet-segment name string next-hop l3-next-hop (ipv4-address ipv6-address)</i>
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

evi start number

Description evi range for this ethernet-segment association

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string next-hop l3-next-hop \(ipv4-address | ipv6-address\) evi start number](#)

Tree [evi](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

Max. Elements 1

start number

Description start of the evi-range for this ethernet-segment

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string next-hop l3-next-hop \(ipv4-address | ipv6-address\) evi start number](#)

Range 1 to 65535

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-down-reason keyword

Description The reason for the ethernet-segment being down in the bgp-instance

Context [system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string oper-down-reason keyword](#)

Tree [oper-down-reason](#)

Options

- admin-disabled
- no-nexthop-address
- no-originating-address
- no-associated-interface
- associated-interface-oper-down
- no-esi

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-esi string

Description	The operational Ethernet Segment Identifier used in the ethernet segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string oper-esi string
Tree	oper-esi
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-multi-homing-mode keyword

Description	Operational Multi-homing mode of the ethernet segment. The state of this leaf can be different than the configured value in cases where the configured value is 'all-active' and the multi-homing mode advertised by the ES peers in the AD per-ES routes is 'single-active'. In this case, the state of this leaf will show 'single-active'.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string oper-multi-homing-mode keyword
Tree	oper-multi-homing-mode
Options	<ul style="list-style-type: none"> • all-active • single-active
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-state keyword

Description	This leaf contains the operational state of ethernet segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable

False

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

routes**Description**

Enter the routes context

Context[system](#) [network-instance](#) [protocols](#) [evpn](#) [ethernet-segments](#) [bgp-instance](#) [id](#)
[reference](#) [ethernet-segment](#) [name](#) [string](#) [routes](#)**Tree**[routes](#)**Configurable**

True

Platforms

7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ethernet-segment

Description	Enter the ethernet-segment context
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string routes ethernet-segment
Tree	ethernet-segment
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

originating-ip keyword

Description	The originating ip-address that the inclusive multicast route will be advertised with in this evpn instance
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string routes ethernet-segment originating-ip keyword
Tree	originating-ip
Default	use-system-ipv4-address
Options	<ul style="list-style-type: none"> • use-system-ipv4-address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

next-hop keyword

Description	The ip-address that will be used as the bgp-next hop for all ES and AD per-ES routes advertised for this Ethernet Segment.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string routes next-hop keyword
Tree	next-hop
Default	use-system-ipv4-address
Options	<ul style="list-style-type: none"> • use-system-ipv4-address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type keyword

Description	Ethernet Segment type.
Context	system network-instance protocols evpn ethernet-segments bgp-instance id reference ethernet-segment name string type keyword

Tree	type
Default	none
Options	<ul style="list-style-type: none"> • none • virtual
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

timers

Description	Enter the timers context
Context	system network-instance protocols evpn ethernet-segments timers
Tree	timers
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

activation-timer *number*

Description	Enter the activation-timer context
Context	system network-instance protocols evpn ethernet-segments timers activation-timer <i>number</i>
Tree	activation-timer
Range	0 to 100
Default	3
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

boot-remaining-time *number*

Description	Indicates the number of seconds remaining for the boot timer to expire.
Context	system network-instance protocols evpn ethernet-segments timers boot-remaining-time <i>number</i>
Tree	boot-remaining-time
Units	seconds
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

boot-start-time *string*

Description	Indicates the time at which the boot timer started.
Context	system network-instance protocols evpn ethernet-segments timers boot-start-time <i>string</i>
Tree	boot-start-time
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

boot-timer *number*

Description	Remaining time before running BGP EVPN multi-homing DF election algorithm
Context	system network-instance protocols evpn ethernet-segments timers boot-timer <i>number</i>
Tree	boot-timer
Range	0 to 6000
Default	10
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ntp

Description	Top-level container for NTP configuration and state
Context	system ntp
Tree	ntp
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enables the system NTP client and indicates that the system should attempt to synchronize the clock
Context	system ntp admin-state <i>keyword</i>
Tree	admin-state

Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

network-instance *reference*

Description	Reference to a configured network-instance
Context	system ntp network-instance reference
Tree	network-instance
Reference	network-instance name string
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details the operational state of the NTP client
Context	system ntp oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
- warm-rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

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

Description	List of NTP servers to use for system clock synchronization
Context	system ntp server address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	server
Configurable	True
Platforms	Supported on all platforms

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

Description	IP address of the NTP server, may be either IPv4 or IPv6
Context	system ntp server address (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	True
Platforms	Supported on all platforms

iburst *boolean*

Description	Indicates whether this server should enable burst synchronization or not iburst, 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

Context	system ntp server address (ipv4-address ipv6-address) iburst <i>boolean</i>
Tree	iburst
Default	false
Configurable	True
Platforms	Supported on all platforms

jitter string

Description	Measurement of the variance in latency on the network
Context	system ntp server address (ipv4-address ipv6-address) jitter <i>string</i>
Tree	jitter
Configurable	False
Platforms	Supported on all platforms

offset string

Description	Estimate of the current time offset from the peer This is the time difference between the local and reference clock.
Context	system ntp server address (ipv4-address ipv6-address) offset <i>string</i>
Tree	offset
Configurable	False
Platforms	Supported on all platforms

poll-interval number

Description	Polling interval of the peer
Context	system ntp server address (ipv4-address ipv6-address) poll-interval <i>number</i>
Tree	poll-interval
Range	16 to 3600
Units	seconds
Configurable	False
Platforms	Supported on all platforms

prefer *boolean*

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
Context	system ntp server address (<i>ipv4-address</i> <i>ipv6-address</i>) prefer <i>boolean</i>
Tree	prefer
Default	false
Configurable	True
Platforms	Supported on all platforms

stratum *number*

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
Context	system ntp server address (<i>ipv4-address</i> <i>ipv6-address</i>) stratum <i>number</i>
Tree	stratum
Configurable	False
Platforms	Supported on all platforms

synchronized (*ipv4-address* | *ipv6-address* | *string*)

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
Context	system ntp synchronized (<i>ipv4-address</i> <i>ipv6-address</i> <i>string</i>)
Tree	synchronized
Configurable	False
Platforms	Supported on all platforms

ra-guard-policy *name string*

Description	List containing RA Guard Policy and parameters
Context	system ra-guard-policy <i>name string</i>
Tree	ra-guard-policy
Configurable	True

Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3
Max. Elements	64

name *string*

Description	RA Guard Policy name
Context	system ra-guard-policy name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

action *keyword*

Description	Describes the RA Guard Policy action for RA Messages matching the specified attributes. RA Messages no matching the specified attributes will be handled in the opposite manner.
Context	system ra-guard-policy name <i>string</i> action <i>keyword</i>
Tree	action
Default	discard
Options	<ul style="list-style-type: none"> • accept • discard
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

advertise-prefix-set *reference*

Description	Reference to a prefix set to match advertised address within RA message
Context	system ra-guard-policy name <i>string</i> advertise-prefix-set <i>reference</i>
Tree	advertise-prefix-set
Reference	routing-policy prefix-set name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

hop-limit *number*

Description	Verifies the minimum advertised hop count limit. If not specified the verification is skipped.
--------------------	--

Context	system ra-guard-policy name <i>string</i> hop-limit <i>number</i>
Tree	hop-limit
Range	1 to 255
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

managed-config-flag *boolean*

Description	Causes the RA Guard policy to match IPv6 RA messages with the M (Managed address) flag set. If not specified the verification is skipped.
Context	system ra-guard-policy name <i>string</i> managed-config-flag <i>boolean</i>
Tree	managed-config-flag
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

other-config-flag *boolean*

Description	Causes the RA Guard policy to match IPv6 RA messages with the O (Other config) flag set. If not specified the verification is skipped.
Context	system ra-guard-policy name <i>string</i> other-config-flag <i>boolean</i>
Tree	other-config-flag
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

router-preference *keyword*

Description	Verifies that the advertised default router preference parameter value is equal to or less than the specified limit. If not specified the verification is skipped.
Context	system ra-guard-policy name <i>string</i> router-preference <i>keyword</i>
Tree	router-preference
Options	<ul style="list-style-type: none"> • high • medium • low
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

source-prefix-set *reference*

Description	Reference to a prefix set to match RA source address. If not specified the verification is skipped.
Context	system ra-guard-policy name <i>string</i> source-prefix-set reference
Tree	source-prefix-set
Reference	routing-policy prefix-set name <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

sflow

Description	Context to configure sFlow Agent parameters and report sFlow state
Context	system sflow
Tree	sflow
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Administratively enable or disable sFlow for the system
Context	system sflow admin-state <i>keyword</i>
Tree	admin-state
Default	disable
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

collector [collector-id](#) *number*

Description	List of sFlow collectors to which sFlow sample data is sent
Context	system sflow collector collector-id <i>number</i>
Tree	collector
Configurable	True
Platforms	Supported on all platforms
Max. Elements	8

collector-id *number*

Description	Specify the collector ID
Context	system sflow collector collector-id number
Range	1 to 8
Configurable	True
Platforms	Supported on all platforms

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

Description	The IP address for an sFlow collector
Context	system sflow collector collector-id number collector-address (ipv4-address ipv6-address)
Tree	collector-address
Configurable	True
Platforms	Supported on all platforms

network-instance *reference*

Description	Reference to a configured network-instance
Context	system sflow collector collector-id number network-instance reference
Tree	network-instance
Reference	network-instance name string
Configurable	True
Platforms	Supported on all platforms

next-hop (*ipv4-address* | *ipv6-address*)

Description	Specifies the active IP next hop used to reach the associated collector
Context	system sflow collector collector-id number next-hop (ipv4-address ipv6-address)
Tree	next-hop
Configurable	False
Platforms	Supported on all platforms

port number

Description	Specifies the destination UDP port number to be used in sFlow packets
Context	system sflow collector collector-id number port number
Tree	port
Default	6343
Configurable	True
Platforms	Supported on all platforms

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

Description	Specifies the IP address to be used as the source address in sFlow packets
Context	system sflow collector collector-id number source-address (ipv4-address ipv6-address)
Tree	source-address
Configurable	True
Platforms	Supported on all platforms

sample-rate number

Description	Specify sFlow sample rate This value is the rate at which traffic will be sampled at a rate of 1:N received packets.
Context	system sflow sample-rate number
Tree	sample-rate
Range	1 to 2000000
Default	10000
Configurable	True
Platforms	Supported on all platforms

sample-size number

Description	Specify sFlow sample size This value specifies the number of bytes the sFlow agent samples from each frame.
Context	system sflow sample-size number
Tree	sample-size
Range	256

Default	256
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	system sflow statistics
Tree	statistics
Configurable	False
Platforms	Supported on all platforms

total-offered-packets *number*

Description	Total number of packets subject to sFlow sampling
Context	system sflow statistics total-offered-packets number
Tree	total-offered-packets
Default	0
Configurable	False
Platforms	Supported on all platforms

total-samples-taken *number*

Description	Total number of sFlow samples taken
Context	system sflow statistics total-samples-taken number
Tree	total-samples-taken
Default	0
Configurable	False
Platforms	Supported on all platforms

total-sent-packets *number*

Description	Total number of sFlow packets sent to collectors
Context	system sflow statistics total-sent-packets number
Tree	total-sent-packets
Default	0

Configurable	False
Platforms	Supported on all platforms

snmp

Description	Top-level container for SNMP configuration and state
Context	system snmp
Tree	snmp
Configurable	True
Platforms	Supported on all platforms

community *string*

Description	Enter the community context
Context	system snmp community <i>string</i>
Tree	community
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

network-instance [name](#) *reference*

Description	List of network-instances to run an SNMP server in
Context	system snmp network-instance name <i>reference</i>
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

[name](#) *reference*

Description	Reference to a configured network-instance
Context	system snmp network-instance name <i>reference</i>
Reference	network-instance name <i>string</i>
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enables the SNMP server in this network-instance
Context	system snmp network-instance name <i>reference</i> admin-state <i>keyword</i>
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details the operational state of the SNMP server
Context	system snmp network-instance name <i>reference</i> oper-state <i>keyword</i>
Tree	oper-state
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 • low-power Component is offline due to insufficient system power • degraded Component or process is in a degraded state

- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
 - waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.
- Configurable** False
- Platforms** Supported on all platforms

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

Description	List of IP addresses for the SNMP server to listen on within the network-instance
Context	system snmp network-instance name reference source-address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	source-address
Default	::
Configurable	True
Platforms	Supported on all platforms

ssh-server

Description	Top-level container for SSH server configuration and state
Context	system ssh-server
Tree	ssh-server
Configurable	True
Platforms	Supported on all platforms

network-instance [name reference](#)

Description	List of network-instances to run an SSH server in
Context	system ssh-server network-instance name reference
Tree	network-instance

Configurable	True
Platforms	Supported on all platforms

name *reference*

Description	Reference to a configured network-instance
Context	system ssh-server network-instance name reference
Reference	network-instance name string
Configurable	True
Platforms	Supported on all platforms

admin-state *keyword*

Description	Enables the SSH server in this network-instance
Context	system ssh-server network-instance name reference admin-state keyword
Tree	admin-state
Options	<ul style="list-style-type: none"> • enable • disable
Configurable	True
Platforms	Supported on all platforms

oper-state *keyword*

Description	Details the operational state of the SSH server
Context	system ssh-server network-instance name reference oper-state keyword
Tree	oper-state
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
- low-power
Component is offline due to insufficient system power
- degraded
Component or process is in a degraded state
- warm-reboot
Component or process is currently warm rebooting
Component or process is currently warm rebooting This state is set during a warm reboot immediately following initiation of the reboot, continuing after startup until the system has completed audit. In this state the system will not accept configuration changes.
- waiting
Component or process is currently waiting
Component or process is currently waiting This state can be set by event handler when the reinvoke-with-delay action is used, and indicates that the event handler is waiting for the provided delay before reinvoking the instance.

Configurable	False
Platforms	Supported on all platforms

protocol-version *number*

Description	Protocol version in use by the SSH server
Context	system ssh-server network-instance name <i>reference</i> protocol-version number
Tree	protocol-version
Configurable	False
Platforms	Supported on all platforms

rate-limit *number*

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
Context	system ssh-server network-instance name <i>reference</i> rate-limit number
Tree	rate-limit
Default	20
Configurable	True
Platforms	Supported on all platforms

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

Description	List of IP addresses for the SSH server to listen on within the network-instance
Context	system ssh-server network-instance name <i>reference</i> source-address (ipv4-address ipv6-address)
Tree	source-address
Configurable	True
Platforms	Supported on all platforms

timeout *number*

Description	Set the idle timeout in seconds on SSH connections
Context	system ssh-server network-instance name <i>reference</i> timeout number
Tree	timeout
Default	0
Units	seconds
Configurable	True
Platforms	Supported on all platforms

tls

Description	Top-level container for TLS configuration and state
Context	system tls
Tree	tls
Configurable	True
Platforms	Supported on all platforms

server-profile *name string*

Description	List of configured TLS server profiles
Context	system tls server-profile name string
Tree	server-profile
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of the TLS server-profile
Context	system tls server-profile name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

authenticate-client *boolean*

Description	Defines if the server should authenticate the identity of connecting clients using the trust anchor
Context	system tls server-profile name string authenticate-client boolean
Tree	authenticate-client
Default	false
Configurable	True
Platforms	Supported on all platforms

certificate *string*

Description	Base64 encoded certificate to use with the private key this includes the '--BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' header and footer
Context	system tls server-profile name string certificate string
Tree	certificate
Configurable	True
Platforms	Supported on all platforms

cipher-list *identityref*

Description	List of ciphers to use when negotiating TLS with clients
Context	system tls server-profile name string cipher-list identityref
Tree	cipher-list
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

Platforms

Supported on all platforms

key string**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

Context[system tls server-profile name string key string](#)**Tree**[key](#)**Configurable**

True

Platforms Supported on all platforms

trust-anchor *string*

Description Base64 encoded certificate to use as a trust anchor This includes the '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' header and footer

Context [system tls server-profile name](#) *string* [trust-anchor](#) *string*

Tree [trust-anchor](#)

Configurable True

Platforms Supported on all platforms

trace-options *keyword*

Description Management server trace options

Context [system trace-options](#) *keyword*

Tree [trace-options](#)

Options

- request
- response
- common

Configurable True

Platforms Supported on all platforms

warm-reboot

Description Top-level container for warm reboot options

Context [system warm-reboot](#)

Tree [warm-reboot](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bgp-max-wait *number*

Description The maximum amount of time that BGP will wait to receive End of RIB markers from all peers and for all address families that were up prior to warm reboot (in all network instances).

After this time elapses BGP declares that convergence has occurred and sends its own EOR markers to its peers.

Context	<code>system warm-reboot bgp-max-wait</code> <i>number</i>
Tree	<code>bgp-max-wait</code>
Range	0 to 3600
Default	600
Units	seconds
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

11 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
+ system-filter
+ ipv4-filter
+ clear
+ entry sequence-id number
+ statistics
+ clear
+ ipv6-filter
+ clear
+ entry sequence-id number
+ statistics
+ clear
```

11.1 acl Descriptions

acl

Description	Top level enclosing container for ACL operational tools
Context	acl
Tree	acl
Configurable	True
Platforms	Supported on all platforms

cpm-filter

Description	List of CPM filters
Context	acl cpm-filter
Tree	cpm-filter
Configurable	True
Platforms	Supported on all platforms

ipv4-filter

Description	List of CPM IPv4 filter rules
Context	acl cpm-filter ipv4-filter
Tree	ipv4-filter
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics of all entries of the filter to zero
Context	acl cpm-filter ipv4-filter clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

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

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

sequence-id *number*

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

statistics

Description	Enter the statistics context
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics associated with this particular entry to zero
Context	acl cpm-filter ipv4-filter entry sequence-id <i>number</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

ipv6-filter

Description	List of CPM IPv6 filter rules
Context	acl cpm-filter ipv6-filter
Tree	ipv6-filter
Configurable	True

Platforms Supported on all platforms

clear

Description Reset all statistics of all entries of the filter to zero

Context [acl cpm-filter ipv6-filter clear](#)

Tree [clear](#)

Configurable True

Platforms Supported on all platforms

entry [sequence-id number](#)

Description List of filter rules.

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

Tree [entry](#)

Configurable True

Platforms Supported on all platforms

sequence-id *number*

Description A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries

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

Configurable True

Platforms Supported on all platforms

statistics

Description Enter the statistics context

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

Tree [statistics](#)

Configurable True

Platforms Supported on all platforms

clear

Description Reset all statistics associated with this particular entry to zero

Context	acl cpm-filter ipv6-filter entry sequence-id number statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

ipv4-filter *name string*

Description	List of IPv4 filter policies
Context	acl ipv4-filter name string
Tree	ipv4-filter
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of the IPv4 filter policy.
Context	acl ipv4-filter name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

entry *sequence-id number*

Description	List of filter rules.
Context	acl ipv4-filter name string entry sequence-id number
Tree	entry
Configurable	True
Platforms	Supported on all platforms

sequence-id *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl ipv4-filter name string entry sequence-id number
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all aggregate and per-interface statistics associated with this particular entry to zero
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

per-interface

Description	Container for per-subinterface per-entry statistics
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Configurable	True
Platforms	Supported on all platforms

subinterface [name](#) *string*

Description	List of subinterfaces where the ACL is applied to either input or output traffic
Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Enter the name context
--------------------	------------------------

Context	acl ipv4-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset the per-interface statistics associated with this particular entry and this particular subinterface to zero
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
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl ipv4-filter name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics of all entries of the filter to zero
Context	acl ipv4-filter name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

ipv6-filter *name string*

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

Configurable	True
Platforms	Supported on all platforms

name *string*

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

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

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

sequence-id *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i>
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all aggregate and per-interface statistics associated with this particular entry to zero
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

per-interface

Description	Container for per-subinterface per-entry statistics
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface
Tree	per-interface
Configurable	True
Platforms	Supported on all platforms

subinterface *name string*

Description	List of subinterfaces where the ACL is applied to either input or output traffic
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
Tree	subinterface
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Enter the name context
Context	acl ipv6-filter name <i>string</i> entry sequence-id <i>number</i> statistics per-interface subinterface name <i>string</i>
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset the per-interface statistics associated with this particular entry and this particular subinterface to zero
--------------------	---

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
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl ipv6-filter name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics of all entries of the filter to zero
Context	acl ipv6-filter name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

policers

Description	List of policers used by ACL entries
Context	acl policers
Tree	policers
Configurable	True
Platforms	Supported on all platforms

policer [name](#) *string*

Description	List of hardware policers
Context	acl policers policer name <i>string</i>
Tree	policer
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Name of the hardware policer
Context	acl policers policer name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl policers policer name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics associated with this particular policer to zero
Context	acl policers policer name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

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

Description	List of system CPU policers
Context	acl policers system-cpu-policer name <i>string</i>
Tree	system-cpu-policer
Configurable	True
Platforms	Supported on all platforms

name *string*

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

Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl policers system-cpu-policer name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics associated with this particular policer to zero
Context	acl policers system-cpu-policer name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

system-filter

Description	List of System filters
Context	acl system-filter
Tree	system-filter
Configurable	True
Platforms	Supported on all platforms

ipv4-filter

Description	List of System IPv4 filter rules
Context	acl system-filter ipv4-filter
Tree	ipv4-filter
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics of all entries of the filter to zero
Context	acl system-filter ipv4-filter clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

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

Description	List of filter rules.
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i>
Tree	entry
Configurable	True
Platforms	Supported on all platforms

[sequence-id](#) *number*

Description	A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i>
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics associated with this particular entry to zero
Context	acl system-filter ipv4-filter entry sequence-id <i>number</i> statistics clear
Tree	clear
Configurable	True

Platforms Supported on all platforms

ipv6-filter

Description List of System IPv6 filter rules
Context [acl system-filter ipv6-filter](#)
Tree [ipv6-filter](#)
Configurable True
Platforms Supported on all platforms

clear

Description Reset all statistics of all entries of the filter to zero
Context [acl system-filter ipv6-filter clear](#)
Tree [clear](#)
Configurable True
Platforms Supported on all platforms

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

Description List of filter rules.
Context [acl system-filter ipv6-filter entry sequence-id number](#)
Tree [entry](#)
Configurable True
Platforms Supported on all platforms

sequence-id *number*

Description A number to indicate the relative evaluation order of the different entries; lower numbered entries are evaluated before higher numbered entries
Context [acl system-filter ipv6-filter entry sequence-id number](#)
Configurable True
Platforms Supported on all platforms

statistics

Description Enter the statistics context

Context	acl system-filter ipv6-filter entry sequence-id number statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all statistics associated with this particular entry to zero
Context	acl system-filter ipv6-filter entry sequence-id number statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

12 tools bfd

```
bfd
+ micro-bfd-sessions
  + lag-interface name string
    + member-interface name string
      + clear
    + statistics
      + lag-interface name string
        + member-interface name string
          + clear
  + peer local-discriminator number
    + clear
+ statistics
  + peer local-discriminator number
    + clear
```

12.1 bfd Descriptions

bfd

Description	Top-level grouping for bfd operational commands
Context	bfd
Tree	bfd
Configurable	True
Platforms	Supported on all platforms

micro-bfd-sessions

Description	Enter the micro-bfd-sessions context
Context	bfd micro-bfd-sessions
Tree	micro-bfd-sessions
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lag-interface [name string](#)

Description	Lag interface against which the clear command is to be executed
Context	bfd micro-bfd-sessions lag-interface name string
Tree	lag-interface
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name [string](#)

Description	Reference ID for associated lag interface Example: lag1 (Reference Interface lag1).
Context	bfd micro-bfd-sessions lag-interface name string
String Length	3 to 132
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

member-interface *name string*

Description	List of member-interfaces to be cleared
Context	bfd micro-bfd-sessions lag-interface name string member-interface name string
Tree	member-interface
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *string*

Description	Reference ID for associated ethernet interface Example: ethernet-2/1 (Reference Interface ethernet-2/1).
Context	bfd micro-bfd-sessions lag-interface name string member-interface name string
String Length	3 to 132
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear the associated micro-BFD sessions Clearing a micro-BFD sessions causes the associated sessions to transition to a Down state
Context	bfd micro-bfd-sessions lag-interface name string member-interface name string clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

statistics

Description	Enter the statistics context
Context	bfd micro-bfd-sessions statistics
Tree	statistics
Configurable	True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

lag-interface *name string*

Description Lag interface against which the clear command is to be executed

Context [bfd micro-bfd-sessions statistics lag-interface name string](#)

Tree [lag-interface](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *string*

Description Reference ID for associated lag interface Example: lag1 (Reference Interface lag1).

Context [bfd micro-bfd-sessions statistics lag-interface name string](#)

String Length 3 to 132

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

member-interface *name string*

Description List of member-interfaces to be cleared

Context [bfd micro-bfd-sessions statistics lag-interface name string member-interface name string](#)

Tree [member-interface](#)

Configurable True

Platforms 7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

name *string*

Description Reference ID for associated ethernet interface Example: ethernet-2/1 (Reference Interface ethernet-2/1).

Context [bfd micro-bfd-sessions statistics lag-interface name string member-interface name string](#)

String Length 3 to 132

Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear the BFD statistics associated with the micro-BFD sessions
Context	bfd micro-bfd-sessions statistics lag-interface name string member-interface name string clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

peer local-discriminator number

Description	The list of local-discriminators associated with BFD
Context	bfd peer local-discriminator number
Tree	peer
Configurable	True
Platforms	Supported on all platforms

local-discriminator number

Description	BFD session local discriminator
Context	bfd peer local-discriminator number
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear the associated BFD sessions Clearing a BFD sessions causes the associated BFD sessions ot transition to a Down state
Context	bfd peer local-discriminator number clear
Tree	clear
Configurable	True

Platforms Supported on all platforms

statistics

Description Enter the statistics context

Context [bfd statistics](#)

Tree [statistics](#)

Configurable True

Platforms Supported on all platforms

peer [local-discriminator number](#)

Description The list of local-discriminators associated with BFD

Context [bfd statistics peer local-discriminator number](#)

Tree [peer](#)

Configurable True

Platforms Supported on all platforms

local-discriminator *number*

Description BFD session local discriminator

Context [bfd statistics peer local-discriminator number](#)

Configurable True

Platforms Supported on all platforms

clear

Description Clear the BFD statistics associated with the BFD sessions

Context [bfd statistics peer local-discriminator number clear](#)

Tree [clear](#)

Configurable True

Platforms Supported on all platforms

13 tools interface

```

interface name string
+ ethernet
+   statistics
+     clear
+     include-members
+ resource
+ retry
+ statistics
+   clear
+   include-members
+ 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
+       duplicate-entries
+         mac address string
+         delete-mac
+     mac-learning
+       delete-all-macs
+       learnt-entries
+         mac address string
+         delete-mac
+   ipv4
+     arp
+       delete-dynamic
+       neighbor ipv4-address string
+         delete-dynamic
+       virtual-ipv4-discovery
+         address ipv4-address string
+         statistics
+           clear
+         statistics
+           clear
+     dhcp-relay
+       statistics
+       clear
+   ipv6
+     dhcp-relay
+       statistics
+       clear
+     neighbor-discovery
+       delete-dynamic
+       neighbor ipv6-address string
+         delete-dynamic
+     virtual-ipv6-discovery
+       address ipv6-address string
+       statistics
+         clear
+       statistics
+         clear
+   statistics

```

+ clear

13.1 interface Descriptions

interface *name string*

Description	The list of named interfaces on the device.
Context	interface name string
Tree	interface
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	References the configured name of the interface
Context	interface name string
Configurable	True
Platforms	Supported on all platforms

ethernet

Description	Enter the ethernet context
Context	interface name string ethernet
Tree	ethernet
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name string ethernet statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear interface ethernet statistics
--------------------	-------------------------------------

Context	interface name <i>string</i> ethernet statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

include-members

Description	Causes the member link ethernet statistics to also be cleared
Context	interface name <i>string</i> ethernet statistics clear include-members
Tree	include-members
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

resource

Description	Enable the resource context
Context	interface name <i>string</i> resource
Tree	resource
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

retry

Description	Causes the specified lag to be reevaluate for missing system resources
Context	interface name <i>string</i> resource retry
Tree	retry
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> statistics
Tree	statistics

Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear interface statistics
Context	interface name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

include-members

Description	Causes the member link statistics to also be cleared
Context	interface name <i>string</i> statistics clear include-members
Tree	include-members
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

queue-statistics

Description	Enter the queue-statistics context
Context	interface name <i>string</i> statistics queue-statistics
Tree	queue-statistics
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Enter the clear context
Context	interface name <i>string</i> statistics queue-statistics clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

multicast-queue *queue-id number*

Description	Enter the multicast-queue list instance
Context	interface name <i>string</i> statistics queue-statistics multicast-queue queue-id number
Tree	multicast-queue
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

queue-id *number*

Description	Queue number: 0-7
Context	interface name <i>string</i> statistics queue-statistics multicast-queue queue-id number
Range	0 to 7
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Enter the clear context
Context	interface name <i>string</i> statistics queue-statistics multicast-queue queue-id number clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

unicast-queue *queue-id number*

Description	Enter the unicast-queue list instance
Context	interface name <i>string</i> statistics queue-statistics unicast-queue queue-id number
Tree	unicast-queue
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

queue-id *number*

Description	Queue number: 0-7
Context	interface name <i>string</i> statistics queue-statistics unicast-queue queue-id <i>number</i>
Range	0 to 7
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Enter the clear context
Context	interface name <i>string</i> statistics queue-statistics unicast-queue queue-id <i>number</i> clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D3L, 7250 IXR-10

subinterface [index](#) *number*

Description	The list of subinterfaces (logical interfaces) associated with a physical interface
Context	interface name <i>string</i> subinterface index <i>number</i>
Tree	subinterface
Configurable	True
Platforms	Supported on all platforms

index *number*

Description	The index of the subinterface, or logical interface number
Context	interface name <i>string</i> subinterface index <i>number</i>
Configurable	True
Platforms	Supported on all platforms

bridge-table

Description	Enter the bridge-table context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table
Tree	bridge-table
Configurable	True
Platforms	Supported on all platforms

mac-duplication

Description	Enable the mac-duplication context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-duplication
Tree	mac-duplication
Configurable	True
Platforms	Supported on all platforms

delete-all-macs

Description	Delete all learnt MAC entries
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-duplication delete-all-macs
Tree	delete-all-macs
Configurable	True
Platforms	Supported on all platforms

duplicate-entries

Description	Enter the duplicate-entries context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> bridge-table mac-duplication duplicate-entries
Tree	duplicate-entries
Configurable	True
Platforms	Supported on all platforms

mac [address](#) *string*

Description	MACs learnt on the bridging instance
--------------------	--------------------------------------

Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Tree	mac
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Enter the address context
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

delete-mac

Description	Delete the duplicate MAC address
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> delete-mac
Tree	delete-mac
Configurable	True
Platforms	Supported on all platforms

mac-learning

Description	Enable the mac-learning context
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning
Tree	mac-learning
Configurable	True
Platforms	Supported on all platforms

delete-all-macs

Description	Delete all learnt MAC entries.
Context	interface name <i>string</i> subinterface index <i>number</i> bridge-table mac-learning delete-all-macs
Tree	delete-all-macs
Configurable	True

Platforms Supported on all platforms

learnt-entries

Description Enter the learnt-entries context

Context [interface name](#) *string* [subinterface](#) *index* *number* [bridge-table](#) [mac-learning](#) [learnt-entries](#)

Tree [learnt-entries](#)

Configurable True

Platforms Supported on all platforms

mac [address](#) *string*

Description MACs learnt on the bridging instance

Context [interface name](#) *string* [subinterface](#) *index* *number* [bridge-table](#) [mac-learning](#) [learnt-entries](#) [mac address](#) *string*

Tree [mac](#)

Configurable True

Platforms Supported on all platforms

address *string*

Description Enter the address context

Context [interface name](#) *string* [subinterface](#) *index* *number* [bridge-table](#) [mac-learning](#) [learnt-entries](#) [mac address](#) *string*

Configurable True

Platforms Supported on all platforms

delete-mac

Description Delete the learnt MAC address.

Context [interface name](#) *string* [subinterface](#) *index* *number* [bridge-table](#) [mac-learning](#) [learnt-entries](#) [mac address](#) *string* [delete-mac](#)

Tree [delete-mac](#)

Configurable True

Platforms Supported on all platforms

ipv4

Description	Enter the ipv4 context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4
Tree	ipv4
Configurable	True
Platforms	Supported on all platforms

arp

Description	Enable the arp context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp
Tree	arp
Configurable	True
Platforms	Supported on all platforms

delete-dynamic

Description	Delete all dynamic ARP entries
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp delete-dynamic
Tree	delete-dynamic
Configurable	True
Platforms	Supported on all platforms

neighbor [ipv4-address](#) *string*

Description	Enter the neighbor list instance
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>
Tree	neighbor
Configurable	True
Platforms	Supported on all platforms

[ipv4-address](#) *string*

Description	IPv4 address resolved by the ARP entry
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i>

Configurable	True
Platforms	Supported on all platforms

delete-dynamic

Description	Delete one specific dynamic ARP entry
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp neighbor ipv4-address <i>string</i> delete-dynamic
Tree	delete-dynamic
Configurable	True
Platforms	Supported on all platforms

virtual-ipv4-discovery

Description	Enter the virtual-ipv4-discovery context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp virtual-ipv4-discovery
Tree	virtual-ipv4-discovery
Configurable	True
Platforms	Supported on all platforms

address [ipv4-address](#) *string*

Description	The list of Virtual IP addresses
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms

[ipv4-address](#) *string*

Description	The virtual IPv4 address.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface index number ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clears the statistics for the Virtual IP addresses
Context	interface name <i>string</i> subinterface index number ipv4 arp virtual-ipv4-discovery address ipv4-address <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface index number ipv4 arp virtual-ipv4-discovery statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clears the global statistics for all the Virtual IP addresses
Context	interface name <i>string</i> subinterface index number ipv4 arp virtual-ipv4-discovery statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

dhcp-relay

Description	Enable the dhcp-relay context
Context	interface name string subinterface index number ipv4 dhcp-relay
Tree	dhcp-relay
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name string subinterface index number ipv4 dhcp-relay statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Enter the clear context
Context	interface name string subinterface index number ipv4 dhcp-relay statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

ipv6

Description	Enter the ipv6 context
Context	interface name string subinterface index number ipv6
Tree	ipv6
Configurable	True
Platforms	Supported on all platforms

dhcp-relay

Description	Enable the dhcp-relay context
Context	interface name string subinterface index number ipv6 dhcp-relay
Tree	dhcp-relay

Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-relay statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Enter the clear context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 dhcp-relay statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

neighbor-discovery

Description	Enable the neighbor-discovery context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery
Tree	neighbor-discovery
Configurable	True
Platforms	Supported on all platforms

delete-dynamic

Description	Delete all dynamic neighbor cache entries
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery delete-dynamic
Tree	delete-dynamic
Configurable	True
Platforms	Supported on all platforms

neighbor ipv6-address *string*

Description	Enter the neighbor list instance
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Tree	neighbor
Configurable	True
Platforms	Supported on all platforms

ipv6-address *string*

Description	IPv6 address resolved by the ND cache entry
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery neighbor ipv6-address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

delete-dynamic

Description	Delete one specific dynamic neighbor cache entry
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
Configurable	True
Platforms	Supported on all platforms

virtual-ipv6-discovery

Description	Enter the virtual-ipv6-discovery context
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery
Tree	virtual-ipv6-discovery
Configurable	True
Platforms	Supported on all platforms

address ipv6-address *string*

Description	The list of Virtual IP addresses
--------------------	----------------------------------

Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i>
Tree	address
Configurable	True
Platforms	Supported on all platforms

ipv6-address *string*

Description	The virtual IPv6 address.
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clears the statistics for the Virtual IP addresses
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery address ipv6-address <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface <i>index</i> <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery statistics
Tree	statistics

Configurable	True
Platforms	Supported on all platforms

clear

Description	Clears the global statistics for all the Virtual IP addresses
Context	interface name <i>string</i> subinterface index <i>number</i> ipv6 neighbor-discovery virtual-ipv6-discovery statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	interface name <i>string</i> subinterface index <i>number</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Enter the clear context
Context	interface name <i>string</i> subinterface index <i>number</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

14 tools network-instance

```

network-instance name string
+ bridge-table
+ mac-duplication
+ delete-macs-type keyword
+ duplicate-entries
+ mac address string
+ delete-mac
+ mac-learning
+ delete-all-macs
+ learnt-entries
+ mac address string
+ delete-mac
+ 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-with-zone)
+ reset-peer
+ soft-clear
+ route-refresh keyword
+ reset-peer
+ peer-as number
+ soft-clear
+ peer-as number
+ route-refresh keyword
+ igmp
+ counters
+ clear
+ interface interface-name string
+ counters
+ clear
+ membership
+ clear
+ group group string
+ clear
+ source source string
+ clear
+ version
+ clear
+ membership
+ clear
+ group group string
+ clear
+ source source string
+ clear
+ version
+ clear
+ isis

```

```
+ instance name string
+ interface interface-name string
  + adjacencies
  + clear
+ ldp-synchronization
  + exit
+ link-state-database
  + clear
+ statistics
  + clear
+ ldp
+ discovery
  + interfaces
    + interface name string
      + ipv4
        + statistics
        + clear
  + peers
    + peer lsr-id string label-space-id number
      + reset
      + statistics
      + clear
+ reset-overload
+ statistics
  + clear
+ ospf
+ instance name string
  + area area-id
    + interface interface-name string
      + neighbors
      + clear
  + ldp-synchronization
  + exit
+ link-state-database
  + clear
+ manual-spf
  + run
+ neighbors
  + clear
  + neighbor neighbor-id
    + clear
+ overload
  + clear
+ statistics
  + clear
```

14.1 network-instance Descriptions

network-instance *name string*

Description	Enter the network-instance list instance
Context	network-instance name string
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	A unique name identifying the network instance
Context	network-instance name string
Configurable	True
Platforms	Supported on all platforms

bridge-table

Description	bridge-table
Context	network-instance name string bridge-table
Tree	bridge-table
Configurable	True
Platforms	Supported on all platforms

mac-duplication

Description	Enable the mac-duplication context
Context	network-instance name string bridge-table mac-duplication
Tree	mac-duplication
Configurable	True
Platforms	Supported on all platforms

delete-macs-type *keyword*

Description	Type of duplicate MAC entries to delete.
--------------------	--

Context	network-instance name <i>string</i> bridge-table mac-duplication delete-macs-type <i>keyword</i>
Tree	delete-macs-type
Options	<ul style="list-style-type: none"> • all • blackhole-only
Configurable	True
Platforms	Supported on all platforms

duplicate-entries

Description	Enter the duplicate-entries context
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries
Tree	duplicate-entries
Configurable	True
Platforms	Supported on all platforms

mac [address](#) *string*

Description	MACs learnt on the bridging instance
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Tree	mac
Configurable	True
Platforms	Supported on all platforms

address *string*

Description	Enter the address context
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i>
Configurable	True
Platforms	Supported on all platforms

delete-mac

Description	Delete the duplicate MAC address.
Context	network-instance name <i>string</i> bridge-table mac-duplication duplicate-entries mac address <i>string</i> delete-mac

Tree	delete-mac
Configurable	True
Platforms	Supported on all platforms

mac-learning

Description	Enable the mac-learning context
Context	network-instance name <i>string</i> bridge-table mac-learning
Tree	mac-learning
Configurable	True
Platforms	Supported on all platforms

delete-all-macs

Description	Delete all learnt MAC entries.
Context	network-instance name <i>string</i> bridge-table mac-learning delete-all-macs
Tree	delete-all-macs
Configurable	True
Platforms	Supported on all platforms

learnt-entries

Description	Enter the learnt-entries context
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries
Tree	learnt-entries
Configurable	True
Platforms	Supported on all platforms

mac *address string*

Description	MACs learnt on the bridging instance
Context	network-instance name <i>string</i> bridge-table mac-learning learnt-entries mac address <i>string</i>
Tree	mac
Configurable	True
Platforms	Supported on all platforms

address string

Description	Enter the address context
Context	network-instance name string bridge-table mac-learning learnt-entries mac address string
Configurable	True
Platforms	Supported on all platforms

delete-mac

Description	Delete the learnt MAC address.
Context	network-instance name string bridge-table mac-learning learnt-entries mac address string delete-mac
Tree	delete-mac
Configurable	True
Platforms	Supported on all platforms

icmp

Description	Enter the icmp context
Context	network-instance name string icmp
Tree	icmp
Configurable	True
Platforms	Supported on all platforms

statistics

Description	ICMP version 4 statistics
Context	network-instance name string icmp statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Resets all the YANG state counters under network-instance/icmp/statistics to zero
--------------------	---

Context	network-instance name <i>string</i> icmp statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

icmp6

Description	Enter the icmp6 context
Context	network-instance name <i>string</i> icmp6
Tree	icmp6
Configurable	True
Platforms	Supported on all platforms

statistics

Description	ICMP version 6 statistics
Context	network-instance name <i>string</i> icmp6 statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Resets all the YANG state counters under network-instance/icmp6/statistics to zero
Context	network-instance name <i>string</i> icmp6 statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

protocols

Description	The routing protocols that are enabled for this network-instance.
Context	network-instance name <i>string</i> protocols
Tree	protocols
Configurable	True
Platforms	Supported on all platforms

bgp

Description	Enable the bgp context
Context	network-instance name <i>string</i> protocols bgp
Tree	bgp
Configurable	True
Platforms	Supported on all platforms

group [group-name](#) *string*

Description	Enter the group list instance
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
Tree	group
Configurable	True
Platforms	Supported on all platforms

group-name *string*

Description	The configured name of the peer group
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

reset-peer

Description	Enable the reset-peer context
Context	network-instance name <i>string</i> protocols bgp group group-name <i>string</i> reset-peer
Tree	reset-peer
Configurable	True
Platforms	Supported on all platforms

peer-as *number*

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
--------------------	--

Context	<code>network-instance name string protocols bgp group group-name string reset-peer peer-as number</code>
Tree	<code>peer-as</code>
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

soft-clear

Description	Enable the soft-clear context
Context	<code>network-instance name string protocols bgp group group-name string soft-clear</code>
Tree	<code>soft-clear</code>
Configurable	True
Platforms	Supported on all platforms

peer-as *number*

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
Context	<code>network-instance name string protocols bgp group group-name string soft-clear peer-as number</code>
Tree	<code>peer-as</code>
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

route-refresh *keyword*

Description	The address family to refresh This is encoded in the ROUTE_REFRESH message. By default all families are refreshed.
Context	<code>network-instance name string protocols bgp group group-name string soft-clear route-refresh keyword</code>
Tree	<code>route-refresh</code>
Options	<ul style="list-style-type: none"> • ipv4-unicast • ipv6-unicast • evpn

Configurable	True
Platforms	Supported on all platforms

neighbor **peer-address** (*ipv4-address | ipv6-address-with-zone*)

Description	Enter the neighbor list instance
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>)
Tree	neighbor
Configurable	True
Platforms	Supported on all platforms

peer-address (*ipv4-address | ipv6-address-with-zone*)

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.
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>)
Configurable	True
Platforms	Supported on all platforms

reset-peer

Description	Hard reset the peer
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) reset-peer
Tree	reset-peer
Configurable	True
Platforms	Supported on all platforms

soft-clear

Description	Enable the soft-clear context
Context	network-instance name <i>string</i> protocols bgp neighbor peer-address (<i>ipv4-address ipv6-address-with-zone</i>) soft-clear
Tree	soft-clear
Configurable	True

Platforms Supported on all platforms

route-refresh *keyword*

Description The address family to refresh
This is encoded in the ROUTE_REFRESH message. By default all families are refreshed.

Context [network-instance name](#) *string* [protocols bgp neighbor peer-address](#) (*ipv4-address | ipv6-address-with-zone*) [soft-clear route-refresh keyword](#)

Tree [route-refresh](#)

Options

- [ipv4-unicast](#)
- [ipv6-unicast](#)
- [evpn](#)

Configurable True

Platforms Supported on all platforms

reset-peer

Description Enable the reset-peer context

Context [network-instance name](#) *string* [protocols bgp reset-peer](#)

Tree [reset-peer](#)

Configurable True

Platforms Supported on all platforms

peer-as *number*

Description Hard reset only BGP peers that have the specified peer-AS number, whether they are configured peers or dynamic peers

Context [network-instance name](#) *string* [protocols bgp reset-peer peer-as](#) *number*

Tree [peer-as](#)

Range 1 to 4294967295

Configurable True

Platforms Supported on all platforms

soft-clear

Description Enable the soft-clear context

Context	network-instance name <i>string</i> protocols bgp soft-clear
Tree	soft-clear
Configurable	True
Platforms	Supported on all platforms

peer-as *number*

Description	Soft reset only BGP peers that have the specified peer-AS number, whether they are configured peers or dynamic peers
Context	network-instance name <i>string</i> protocols bgp soft-clear peer-as <i>number</i>
Tree	peer-as
Range	1 to 4294967295
Configurable	True
Platforms	Supported on all platforms

route-refresh *keyword*

Description	The address family to refresh This is encoded in the ROUTE_REFRESH message. By default all families are refreshed.
Context	network-instance name <i>string</i> protocols bgp soft-clear route-refresh <i>keyword</i>
Tree	route-refresh
Options	<ul style="list-style-type: none"> • ipv4-unicast • ipv6-unicast • evpn
Configurable	True
Platforms	Supported on all platforms

igmp

Description	Enable the igmp context
Context	network-instance name <i>string</i> protocols igmp
Tree	igmp
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

counters

Description	Enter the counters context
Context	network-instance name <i>string</i> protocols igmp counters
Tree	counters
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Reset IGMP counters for all interfaces.
Context	network-instance name <i>string</i> protocols igmp counters clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interface [interface-name](#) *string*

Description	List of IGMP interfaces
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>string</i>
Tree	interface
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

interface-name *string*

Description	Reference to a specific subinterface of the form <interface-name>.<subinterface-index>
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>string</i>
String Length	5 to 137
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

counters

Description	Enter the counters context
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>string</i> counters
Tree	counters
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Reset IGMP counters for this interface.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>string</i> counters clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

membership

Description	Enter the membership context
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>string</i> membership
Tree	membership
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear all IGMP memberships for this interface.
Context	network-instance name <i>string</i> protocols igmp interface interface-name <i>string</i> membership clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group *group string*

Description	Multicast group membership.
Context	network-instance name string protocols igmp interface interface-name string membership group group string
Tree	group
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group *string*

Description	Multicast address.
Context	network-instance name string protocols igmp interface interface-name string membership group group string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear all IGMP memberships for this group on this interface.
Context	network-instance name string protocols igmp interface interface-name string membership group group string clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source *source string*

Description	Source addresses of multicast.
Context	network-instance name string protocols igmp interface interface-name string membership group group string source source string
Tree	source
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source string

Description	Source address of multicast.
Context	network-instance name string protocols igmp interface interface-name string membership group group string source source string
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear all IGMP memberships for this group on this interface.
Context	network-instance name string protocols igmp interface interface-name string membership group group string source source string clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

version

Description	Enter the version context
Context	network-instance name string protocols igmp interface interface-name string version
Tree	version
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Reset the IGMP operational version for this interface.
Context	network-instance name string protocols igmp interface interface-name string version clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

membership

Description	Enter the membership context
Context	network-instance name <i>string</i> protocols igmp membership
Tree	membership
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear the IGMP memberships for all interfaces.
Context	network-instance name <i>string</i> protocols igmp membership clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group [group](#) *string*

Description	Multicast group membership.
Context	network-instance name <i>string</i> protocols igmp membership group group <i>string</i>
Tree	group
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

group *string*

Description	Multicast address.
Context	network-instance name <i>string</i> protocols igmp membership group group <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear all IGMP memberships for this group on all interfaces.
--------------------	--

Context	network-instance name <i>string</i> protocols igmp membership group group <i>string</i> clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source [source](#) *string*

Description	Source addresses of multicast.
Context	network-instance name <i>string</i> protocols igmp membership group group <i>string</i> source source <i>string</i>
Tree	source
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

source *string*

Description	Source address of multicast.
Context	network-instance name <i>string</i> protocols igmp membership group group <i>string</i> source source <i>string</i>
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Clear all IGMP memberships for this group on all interfaces.
Context	network-instance name <i>string</i> protocols igmp membership group group <i>string</i> source source <i>string</i> clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

version

Description	Enter the version context
--------------------	---------------------------

Context	network-instance name <i>string</i> protocols igmp version
Tree	version
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

clear

Description	Reset the IGMP operational version for all interfaces.
Context	network-instance name <i>string</i> protocols igmp version clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7250 IXR-6, 7220 IXR-D3, 7220 IXR-D2, 7220 IXR-H3, 7220 IXR-H2, 7220 IXR-D1, 7220 IXR-D3L, 7250 IXR-10

isis

Description	Enable the isis context
Context	network-instance name <i>string</i> protocols isis
Tree	isis
Configurable	True
Platforms	Supported on all platforms

instance [name](#) *string*

Description	List of IS-IS protocol instances associated with this network-instance. Only a single instance is supported for now
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>
Tree	instance
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

name *string*

Description	The name of the IS-IS instance
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i>

String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

interface *interface-name string*

Description	List of IS-IS interfaces
Context	network-instance name string protocols isis instance name string interface interface-name string
Tree	interface
Configurable	True
Platforms	Supported on all platforms

interface-name *string*

Description	Reference to a specific subinterface of the form <interface-name>.<subinterface-index>
Context	network-instance name string protocols isis instance name string interface interface-name string
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

adjacencies

Description	Enter the adjacencies context
Context	network-instance name string protocols isis instance name string interface interface-name string adjacencies
Tree	adjacencies
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all of the adjacencies on this interface
Context	network-instance name string protocols isis instance name string interface interface-name string adjacencies clear
Tree	clear

Configurable	True
Platforms	Supported on all platforms

ldp-synchronization

Description	IS-IS LDP-IGP synchronisation
Context	network-instance name string protocols isis instance name string ldp-synchronization
Tree	ldp-synchronization
Configurable	True
Platforms	Supported on all platforms

exit

Description	Advertise the normal metric for all IS-IS interfaces, even if some are configured for LDP synchronization and ISIS is not in sync with LDP on these interfaces
Context	network-instance name string protocols isis instance name string ldp-synchronization exit
Tree	exit
Configurable	True
Platforms	Supported on all platforms

link-state-database

Description	The ISIS link state database
Context	network-instance name string protocols isis instance name string link-state-database
Tree	link-state-database
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear the contents of the LSDB.
Context	network-instance name string protocols isis instance name string link-state-database clear
Tree	clear

Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all of the IS-IS instance statistics to zero.
Context	network-instance name <i>string</i> protocols isis instance name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

ldp

Description	Operational tools commands for LDP.
Context	network-instance name <i>string</i> protocols ldp
Tree	ldp
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

discovery

Description	Enter the discovery context
Context	network-instance name <i>string</i> protocols ldp discovery
Tree	discovery
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

interfaces

Description	Enter the interfaces context
Context	network-instance name <i>string</i> protocols ldp discovery interfaces
Tree	interfaces
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

interface *name string*

Description	Enter the interface list instance
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>string</i>
Tree	interface
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

name *string*

Description	Reference type to a specific subinterface of the form <interface-name>.<subinterface-index>
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>string</i>
String Length	5 to 25
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ipv4

Description	Enter the ipv4 context
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>string</i> ipv4
Tree	ipv4
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Enter the statistics context
--------------------	------------------------------

Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>string</i> ipv4 statistics
Tree	statistics
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

clear

Description	Resets all the LDP instance state counters to zero
Context	network-instance name <i>string</i> protocols ldp discovery interfaces interface name <i>string</i> ipv4 statistics clear
Tree	clear
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

peers

Description	Enter the peers context
Context	network-instance name <i>string</i> protocols ldp peers
Tree	peers
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

peer *lsr-id string label-space-id number*

Description	List of peers.
Context	network-instance name <i>string</i> protocols ldp peers peer <i>lsr-id string label-space-id number</i>
Tree	peer
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

lsr-id *string*

Description	The LSR ID of the peer, to identify the globally unique LSR. This is the first four octets of the LDP ID. This leaf is used together with the leaf 'label-space-id' to form the LDP ID.
--------------------	---

Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

label-space-id *number*

Description	The Label Space ID of the peer, to identify a specific label space within the LSR. This is the last two octets of the LDP ID. This leaf is used together with the leaf 'lsr-id' to form the LDP ID.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i>
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

reset

Description	Reset the LDP session by closing the TCP connection and establishing a new one.
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> reset
Tree	reset
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics
Tree	statistics
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

clear

Description	Resets all the LDP instance state counters to zero
Context	network-instance name <i>string</i> protocols ldp peers peer lsr-id <i>string</i> label-space-id <i>number</i> statistics clear

Tree	clear
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

reset-overload

Description	Enable the reset-overload context
Context	network-instance name <i>string</i> protocols ldp reset-overload
Tree	reset-overload
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> protocols ldp statistics
Tree	statistics
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

clear

Description	Resets all the LDP instance state counters to zero
Context	network-instance name <i>string</i> protocols ldp statistics clear
Tree	clear
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

ospf

Description	Enable the ospf context
Context	network-instance name <i>string</i> protocols ospf
Tree	ospf
Configurable	True
Platforms	Supported on all platforms

instance *name string*

Description	List of OSPF protocol instances associated with this network-instance. Only a single instance is supported for now
Context	<i>network-instance name string protocols ospf instance name string</i>
Tree	<i>instance</i>
Configurable	True
Platforms	Supported on all platforms
Max. Elements	1

name *string*

Description	The name of the OSPF instance
Context	<i>network-instance name string protocols ospf instance name string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

area *area-id*

Description	List of OSPF area
Context	<i>network-instance name string protocols ospf instance name string area area-id</i>
Tree	<i>area</i>
Configurable	True
Platforms	Supported on all platforms

area-id

Description	Enter the area-id context
Context	<i>network-instance name string protocols ospf instance name string area area-id</i>
Configurable	True
Platforms	Supported on all platforms

interface *interface-name string*

Description	List of OSPF interfaces
--------------------	-------------------------

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>string</i>
Tree	interface
Configurable	True
Platforms	Supported on all platforms

interface-name *string*

Description	Reference to a specific subinterface of the form <interface-name>.<subinterface-index>
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>string</i>
String Length	5 to 137
Configurable	True
Platforms	Supported on all platforms

neighbors

Description	Enter the neighbors context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>string</i> neighbors
Tree	neighbors
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all of the adjacencies on this interface
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> area area-id interface interface-name <i>string</i> neighbors clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

ldp-synchronization

Description	Enter the ldp-synchronization context
--------------------	---------------------------------------

Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> ldp-synchronization
Tree	ldp-synchronization
Configurable	True
Platforms	Supported on all platforms

exit

Description	Advertise the normal metric for all OSPF interfaces, even if some are configured for LDP synchronization and OSPF is not in sync with LDP on these interfaces
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> ldp-synchronization exit
Tree	exit
Configurable	True
Platforms	Supported on all platforms

link-state-database

Description	The OSPF link state database
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> link-state-database
Tree	link-state-database
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear the contents of the LSDB.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> link-state-database clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

manual-spf

Description	Enter the manual-spf context
--------------------	------------------------------

Context	<code>network-instance name string protocols ospf instance name string manual-spf</code>
Tree	<code>manual-spf</code>
Configurable	True
Platforms	Supported on all platforms

run

Description	Run a SPF calculation.
Context	<code>network-instance name string protocols ospf instance name string manual-spf run</code>
Tree	<code>run</code>
Configurable	True
Platforms	Supported on all platforms

neighbors

Description	Container for OSPF neighbors tools
Context	<code>network-instance name string protocols ospf instance name string neighbors</code>
Tree	<code>neighbors</code>
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear all OSPF neighbors
Context	<code>network-instance name string protocols ospf instance name string neighbors clear</code>
Tree	<code>clear</code>
Configurable	True
Platforms	Supported on all platforms

neighbor neighbor-id

Description	Enter the neighbor list instance
Context	<code>network-instance name string protocols ospf instance name string neighbors neighbor neighbor-id</code>
Tree	<code>neighbor</code>

Configurable	True
Platforms	Supported on all platforms

neighbor-id

Description	The neighbor's ip-address in case of OSPFv2, the router-id otherwise
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> neighbors neighbor neighbor-id
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset this neighbor in the OSPF instance
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> neighbors neighbor neighbor-id clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

overload

Description	Enter the overload context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload
Tree	overload
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset OSPF instance overload status.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> overload clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Reset all of the OSPF instance statistics to zero.
Context	network-instance name <i>string</i> protocols ospf instance name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

15 tools platform

```
platform
+ chassis
+   reboot
+     force
+     warm
+       force
+       validate
+ 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
```

15.1 platform Descriptions

platform

Description	Top-level container for platform operational commands
Context	platform
Tree	platform
Configurable	True
Platforms	Supported on all platforms

chassis

Description	Operational commands related to the chassis
Context	platform chassis
Tree	chassis
Configurable	True
Platforms	Supported on all platforms

reboot

Description	Trigger a reboot of the chassis
Context	platform chassis reboot
Tree	reboot
Configurable	True
Platforms	Supported on all platforms

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
Context	platform chassis reboot force
Tree	force
Configurable	True
Platforms	Supported on all platforms

warm

Description	Perform a warm reboot of the system This option will perform checks against the current configuration, before prompting to confirm the reboot, and then rebooting the system without impacting the datapath - if a new image has been configured, this will upgrade the system.
Context	platform chassis reboot warm
Tree	warm
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

force

Description	Force a warm reboot of the system, overriding any validation, synchronizations or other activities in progress This option can be dangerous, and may result in an outage - but can be used to support a fast reboot of the system.
Context	platform chassis reboot warm force
Tree	force
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

validate

Description	Validate that the system's current configuration and state supports a warm reboot operation
Context	platform chassis reboot warm validate
Tree	validate
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

control [slot string](#)

Description	Operational commands related to control modules
Context	platform control slot string
Tree	control
Configurable	True

Platforms Supported on all platforms

slot *string*

Description Slot identifier for the control module
Context [platform control slot *string*](#)
Configurable True
Platforms Supported on all platforms

locator

Description Operational commands for the locator LED
Context [platform control slot *string* locator](#)
Tree [locator](#)
Configurable True
Platforms Supported on all platforms

disable

Description Deactivates the locator LED for this component
Context [platform control slot *string* locator disable](#)
Tree [disable](#)
Configurable True
Platforms Supported on all platforms

enable

Description Activate the locator LED for this component
Context [platform control slot *string* locator enable](#)
Tree [enable](#)
Configurable True
Platforms Supported on all platforms

duration *number*

Description Sets the duration to activate the locator LED, after which it will disable automatically

Context	platform control slot <i>string</i> locator enable duration <i>number</i>
Tree	duration
Range	10 to 3600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

reboot

Description	Trigger a reboot of the control module
Context	platform control slot <i>string</i> reboot
Tree	reboot
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

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
Context	platform control slot <i>string</i> reboot force
Tree	force
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

[fabric slot](#) *number*

Description	Operational commands related to fabric modules
Context	platform fabric slot <i>number</i>
Tree	fabric
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

[slot](#) *number*

Description	Numeric identifier for the fabric module
--------------------	--

Context	platform fabric slot number
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

locator

Description	Operational commands for the locator LED
Context	platform fabric slot number locator
Tree	locator
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

disable

Description	Deactivates the locator LED for this component
Context	platform fabric slot number locator disable
Tree	disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

enable

Description	Activate the locator LED for this component
Context	platform fabric slot number locator enable
Tree	enable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

duration *number*

Description	Sets the duration to activate the locator LED, after which it will disable automatically
Context	platform fabric slot number locator enable duration number
Tree	duration
Range	10 to 3600
Units	seconds
Configurable	True

Platforms 7250 IXR-10, 7250 IXR-6

reboot

Description Reboot this component
Context [platform fabric slot number reboot](#)
Tree [reboot](#)
Configurable True
Platforms 7250 IXR-10, 7250 IXR-6

fan-tray id number

Description Operational commands related to fan modules
Context [platform fan-tray id number](#)
Tree [fan-tray](#)
Configurable True
Platforms Supported on all platforms

id number

Description Numeric identifier for the fan module
Context [platform fan-tray id number](#)
Configurable True
Platforms Supported on all platforms

locator

Description Operational commands for the locator LED
Context [platform fan-tray id number locator](#)
Tree [locator](#)
Configurable True
Platforms Supported on all platforms

disable

Description Deactivates the locator LED for this component
Context [platform fan-tray id number locator disable](#)

Tree	disable
Configurable	True
Platforms	Supported on all platforms

enable

Description	Activate the locator LED for this component
Context	platform fan-tray id number locator enable
Tree	enable
Configurable	True
Platforms	Supported on all platforms

duration *number*

Description	Sets the duration to activate the locator LED, after which it will disable automatically
Context	platform fan-tray id number locator enable duration number
Tree	duration
Range	10 to 3600
Units	seconds
Configurable	True
Platforms	Supported on all platforms

linecard [slot number](#)

Description	Operational commands related to line cards
Context	platform linecard slot number
Tree	linecard
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

slot *number*

Description	Numeric identifier for the line card
Context	platform linecard slot number
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

locator

Description	Operational commands for the locator LED
Context	platform linecard slot number locator
Tree	locator
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

disable

Description	Deactivates the locator LED for this component
Context	platform linecard slot number locator disable
Tree	disable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

enable

Description	Activate the locator LED for this component
Context	platform linecard slot number locator enable
Tree	enable
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

duration *number*

Description	Sets the duration to activate the locator LED, after which it will disable automatically
Context	platform linecard slot number locator enable duration number
Tree	duration
Range	10 to 3600
Units	seconds
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

reboot

Description	Reboot this component
Context	platform linecard slot <i>number</i> reboot
Tree	reboot
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

redundancy

Description	Top-level container for redundancy operational commands
Context	platform redundancy
Tree	redundancy
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

switchover

Description	Trigger a redundancy switchover to the other control module
Context	platform redundancy switchover
Tree	switchover
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

synchronize

Description	Top-level container for manual synchronization activities
Context	platform redundancy synchronize
Tree	synchronize
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

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
--------------------	---

Context	platform redundancy synchronize overlay
Tree	overlay
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

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
Context	platform redundancy synchronize system
Tree	system
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

show-fabric-bandwidth

Description	Show fabric bandwidth
Context	platform show-fabric-bandwidth
Tree	show-fabric-bandwidth
Configurable	True
Platforms	7250 IXR-10, 7250 IXR-6

16 tools system

```

system
+ aaa
  + authentication
    + session id number
    + disconnect
+ app-management
  + application name string
  + kill
  + quit
  + reload
  + restart
    + cold
    + warm
  + start
  + statistics
  + clear
  + stop
+ boot
+ cgroup
+ configuration
  + candidate name string
  + clear
  + checkpoint id (number | checkpoint-name)
  + clear
  + load
  + revert
  + confirmed-accept
  + confirmed-reject
  + generate-checkpoint
  + comment string
  + name string
  + rescue-clear
  + rescue-save
  + save
  + session id number
  + clear
  + upgrade
  + checkpoint id (number | checkpoint-name)
  + file string
  + rescue
  + startup
+ dhcp-server
  + network-instance name string
  + dhcpv4
    + statistics
    + clear
  + dhcpv6
    + statistics
    + clear
+ event-handler
  + instance name string
  + reload
  + statistics
  + clear
+ l2cp-transparency
  + dot1x
  + clear
  + l2cp-total-statistics

```

```
+ clear
+ lacp
+ clear
+ lldp
+ clear
+ ptp
+ clear
+ xstp
+ clear
+ packet-trace-base64
+ interface string
+ packet binary
+ sync
+ 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
```

16.1 system Descriptions

system

Description	Enclosing container for system management.
Context	system
Tree	system
Configurable	True
Platforms	Supported on all platforms

aaa

Description	Top-level container for operational commands related to aaa
Context	system aaa
Tree	aaa
Configurable	True
Platforms	Supported on all platforms

authentication

Description	Operational commands related to authentication
Context	system aaa authentication
Tree	authentication
Configurable	True
Platforms	Supported on all platforms

session id *number*

Description	List of active sessions in the system
Context	system aaa authentication session id number
Tree	session
Configurable	True
Platforms	Supported on all platforms

id number

Description	System generated session ID
Context	system aaa authentication session id number
Configurable	True
Platforms	Supported on all platforms

disconnect

Description	Disconnect the cli session, requesting the cli to terminate
Context	system aaa authentication session id number disconnect
Tree	disconnect
Configurable	True
Platforms	Supported on all platforms

app-management

Description	Operational commands related to app-management
Context	system app-management
Tree	app-management
Configurable	True
Platforms	Supported on all platforms

application name string

Description	List of all applications managed by the application manager
Context	system app-management application name string
Tree	application
Configurable	True
Platforms	Supported on all platforms

name string

Description	Unique name of this application instance
Context	system app-management application name string
Configurable	True
Platforms	Supported on all platforms

kill

Description	Terminate the application instance ungracefully
Context	system app-management application name <i>string</i> kill
Tree	kill
Configurable	True
Platforms	Supported on all platforms

quit

Description	Terminate the application instance, requesting it to core dump
Context	system app-management application name <i>string</i> quit
Tree	quit
Configurable	True
Platforms	Supported on all platforms

reload

Description	Reload the configuration of the application instance
Context	system app-management application name <i>string</i> reload
Tree	reload
Configurable	True
Platforms	Supported on all platforms

restart

Description	<p>Restart the application instance</p> <p>The best restart that is supported by the application is used if neither 'warm' or 'cold' is specified. If 'warm' restart is supported that will be used, or 'cold' if 'warm' is unavailable.</p> <p>A 'warm' restart will result in the application leaving its state in IDB during the restart, and recovering it post restart. This restart type results in less disruption to surrounding applications that would depend on the restarting applications state.</p> <p>A 'cold' restart will result in a normal stop/start of the application, including the purging of its state in IDB.</p>
Context	system app-management application name <i>string</i> restart
Tree	restart

Configurable	True
Platforms	Supported on all platforms

cold

Description	Perform a cold restart of the application instance
Context	system app-management application name <i>string</i> restart cold
Tree	cold
Configurable	True
Platforms	Supported on all platforms

warm

Description	Perform a warm restart of the application instance
Context	system app-management application name <i>string</i> restart warm
Tree	warm
Configurable	True
Platforms	Supported on all platforms

start

Description	Start the application instance
Context	system app-management application name <i>string</i> start
Tree	start
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Top-level grouping of operational commands related to application statistics
Context	system app-management application name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear statistics for this application instance
Context	system app-management application name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

stop

Description	Terminate the application instance gracefully
Context	system app-management application name <i>string</i> stop
Tree	stop
Configurable	True
Platforms	Supported on all platforms

boot

Description	Top-level container for operational commands related to booting the system
Context	system boot
Tree	boot
Configurable	True
Platforms	Supported on all platforms

cgroup

Description	Top-level container for query commands related to cgroup in the system
Context	system cgroup
Tree	cgroup
Configurable	True
Platforms	Supported on all platforms

configuration

Description	Top-level container for operational commands related to the system configuration
Context	system configuration

Tree	configuration
Configurable	True
Platforms	Supported on all platforms

candidate name string

Description	List of configuration candidates currently active
Context	system configuration candidate name string
Tree	candidate
Configurable	True
Platforms	Supported on all platforms

name string

Description	The name of the candidate
Context	system configuration candidate name string
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

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.
Context	system configuration candidate name string clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

checkpoint id (number | checkpoint-name)

Description	List of current checkpoints present in the system
Context	system configuration checkpoint id (number checkpoint-name)
Tree	checkpoint
Configurable	True
Platforms	Supported on all platforms

id (*number | checkpoint-name*)

Description	System generated ID, or operator defined name for the checkpoint
Context	system configuration checkpoint id (<i>number checkpoint-name</i>)
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear the checkpoint from the system
Context	system configuration checkpoint id (<i>number checkpoint-name</i>) clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

load

Description	Load candidate from saved checkpoint configuration
Context	system configuration checkpoint id (<i>number checkpoint-name</i>) load
Tree	load
Configurable	True
Platforms	Supported on all platforms

revert

Description	Revert running system configuration to the saved checkpoint configuration This functions as a load and commit action.
Context	system configuration checkpoint id (<i>number checkpoint-name</i>) revert
Tree	revert
Configurable	True
Platforms	Supported on all platforms

confirmed-accept

Description	Accepts an in progress commit and stops the confirmation timer
Context	system configuration confirmed-accept

Tree	confirmed-accept
Configurable	True
Platforms	Supported on all platforms

confirmed-reject

Description	Rejects an in progress commit and stops the confirmation timer
Context	system configuration confirmed-reject
Tree	confirmed-reject
Configurable	True
Platforms	Supported on all platforms

generate-checkpoint

Description	Generate a checkpoint point based on the current running configuration
Context	system configuration generate-checkpoint
Tree	generate-checkpoint
Configurable	True
Platforms	Supported on all platforms

comment *string*

Description	User provided comment to associate with the checkpoint
Context	system configuration generate-checkpoint comment <i>string</i>
Tree	comment
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	User provided name of the checkpoint
Context	system configuration generate-checkpoint name <i>string</i>
Tree	name
Configurable	True
Platforms	Supported on all platforms

rescue-clear

Description	Remove rescue configuration
Context	system configuration rescue-clear
Tree	rescue-clear
Configurable	True
Platforms	Supported on all platforms

rescue-save

Description	Save current running configuration as rescue configuration - rescue-config.json
Context	system configuration rescue-save
Tree	rescue-save
Configurable	True
Platforms	Supported on all platforms

save

Description	Save current running configuration as initial (startup) configuration - config.json
Context	system configuration save
Tree	save
Configurable	True
Platforms	Supported on all platforms

session id *number*

Description	List of configuration sessions currently active
Context	system configuration session id <i>number</i>
Tree	session
Configurable	True
Platforms	Supported on all platforms

id *number*

Description	System generated ID for the configuration session
Context	system configuration session id <i>number</i>

Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear the session from the system, discarding any changes
Context	system configuration session id number clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

upgrade

Description	Operational commands related to configuration upgrade
Context	system configuration upgrade
Tree	upgrade
Configurable	True
Platforms	Supported on all platforms

checkpoint id (*number | checkpoint-name*)

Description	List of configuration checkpoints
Context	system configuration upgrade checkpoint id (number checkpoint-name)
Tree	checkpoint
Configurable	True
Platforms	Supported on all platforms

id (*number | checkpoint-name*)

Description	System generated ID, or operator defined name for the checkpoint
Context	system configuration upgrade checkpoint id (number checkpoint-name)
Configurable	True
Platforms	Supported on all platforms

file *string*

Description	System file path to a json configuration file
--------------------	---

Context	system configuration upgrade file <i>string</i>
Tree	file
Configurable	True
Platforms	Supported on all platforms

rescue

Description	Rescue configuration
Context	system configuration upgrade rescue
Tree	rescue
Configurable	True
Platforms	Supported on all platforms

startup

Description	Startup (initial) configuration
Context	system configuration upgrade startup
Tree	startup
Configurable	True
Platforms	Supported on all platforms

dhcp-server

Description	Enable the dhcp-server context
Context	system dhcp-server
Tree	dhcp-server
Configurable	True
Platforms	Supported on all platforms

network-instance [name](#) *string*

Description	List of network instances to run a dhcp server in
Context	system dhcp-server network-instance name <i>string</i>
Tree	network-instance
Configurable	True
Platforms	Supported on all platforms

name *string*

Description	Network Instance
Context	system dhcp-server network-instance name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

dhcpv4

Description	Enter the dhcpv4 context
Context	system dhcp-server network-instance name <i>string</i> dhcpv4
Tree	dhcpv4
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	system dhcp-server network-instance name <i>string</i> dhcpv4 statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Enter the clear context
Context	system dhcp-server network-instance name <i>string</i> dhcpv4 statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

dhcpv6

Description	Enter the dhcpv6 context
Context	system dhcp-server network-instance name <i>string</i> dhcpv6
Tree	dhcpv6

Configurable	True
Platforms	Supported on all platforms

statistics

Description	Enter the statistics context
Context	system dhcp-server network-instance name <i>string</i> dhcpv6 statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Enter the clear context
Context	system dhcp-server network-instance name <i>string</i> dhcpv6 statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

event-handler

Description	Top-level container for operational commands on event handler and event handling instances
Context	system event-handler
Tree	event-handler
Configurable	True
Platforms	Supported on all platforms

instance [name](#) *string*

Description	List of all event handler instances
Context	system event-handler instance name <i>string</i>
Tree	instance
Configurable	True
Platforms	Supported on all platforms
Max. Elements	20

name *string*

Description	A user-defined name for this event handler instance
Context	system event-handler instance name <i>string</i>
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

reload

Description	Reload the Python script for this event handler instance
Context	system event-handler instance name <i>string</i> reload
Tree	reload
Configurable	True
Platforms	Supported on all platforms

statistics

Description	Top-level container for operational commands on event handler statistics
Context	system event-handler instance name <i>string</i> statistics
Tree	statistics
Configurable	True
Platforms	Supported on all platforms

clear

Description	Clear statistics for this event handler instance
Context	system event-handler instance name <i>string</i> statistics clear
Tree	clear
Configurable	True
Platforms	Supported on all platforms

l2cp-transparency

Description	Enable the l2cp-transparency context
Context	system l2cp-transparency

Tree	l2cp-transparency
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

dot1x

Description	Enter the dot1x context
Context	system l2cp-transparency dot1x
Tree	dot1x
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

clear

Description	Clears the statistics for the 802.1x Port based Network Access Control protocol.
Context	system l2cp-transparency dot1x clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

l2cp-total-statistics

Description	Enter the l2cp-total-statistics context
Context	system l2cp-transparency l2cp-total-statistics
Tree	l2cp-total-statistics
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

clear

Description	Clears the global statistics for the L2CP protocols.
Context	system l2cp-transparency l2cp-total-statistics clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lACP

Description	Enter the lACP context
Context	system l2cp-transparency lACP
Tree	lACP
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

clear

Description	Clears the statistics for Link Aggregation Control Protocol.
Context	system l2cp-transparency lACP clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

lLDP

Description	Enter the lLDP context
Context	system l2cp-transparency lLDP
Tree	lLDP
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

clear

Description	Clears the statistics for Link Layer Discovery Protocol.
Context	system l2cp-transparency lLDP clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

ptp

Description	Enter the ptp context
Context	system l2cp-transparency ptp
Tree	ptp

Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

clear

Description	Clears the statistics for the Precision Time Protocol .
Context	system l2cp-transparency ptp clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

xstp

Description	Enter the xstp context
Context	system l2cp-transparency xstp
Tree	xstp
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

clear

Description	Clears the statistics for all the Spanning Tree Protocols.
Context	system l2cp-transparency xstp clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D1, 7220 IXR-D3

packet-trace-base64

Description	Tools command to report the forwarding behavior for a specified test packet (packet specified in base64 format)
Context	system packet-trace-base64
Tree	packet-trace-base64
Configurable	True
Platforms	Supported on all platforms

interface *string*

Description	References the configured name of the interface in which to inject the probe packet
Context	system packet-trace-base64 interface <i>string</i>
Tree	interface
Configurable	True
Platforms	Supported on all platforms

packet *binary*

Description	Packet content encoded in base64 string format
Context	system packet-trace-base64 packet <i>binary</i>
Tree	packet
Configurable	True
Platforms	Supported on all platforms

sync

Description	Top-level grouping for sync operational commands
Context	system sync
Tree	sync
Configurable	True
Platforms	Supported on all platforms

tls

Description	Top-level container for operational commands related to TLS
Context	system tls
Tree	tls
Configurable	True
Platforms	Supported on all platforms

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.

Context	system tls generate-csr
Tree	generate-csr
Configurable	True
Platforms	Supported on all platforms

common-name *string*

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.
Context	system tls generate-csr common-name <i>string</i>
Tree	common-name
String Length	1 to 64
Configurable	True
Platforms	Supported on all platforms

country *string*

Description	The country name to use for the certificate signing request The expected format is two characters long, e.g. 'US'.
Context	system tls generate-csr country <i>string</i>
Tree	country
String Length	2
Default	US
Configurable	True
Platforms	Supported on all platforms

email *string*

Description	The email address to use for the certificate signing request
Context	system tls generate-csr email <i>string</i>
Tree	email
String Length	1 to 255
Configurable	True

Platforms Supported on all platforms

locality string

Description The city or locality to use for the certificate signing request

Context [system tls generate-csr locality string](#)

Tree [locality](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

organization string

Description The organization to use for the certificate signing request

Context [system tls generate-csr organization string](#)

Tree [organization](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

organization-unit string

Description The organization unit to use for the certificate signing request

Context [system tls generate-csr organization-unit string](#)

Tree [organization-unit](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

state string

Description The state or province to use for the certificate signing request

Context [system tls generate-csr state string](#)

Tree [state](#)

String Length 1 to 255

Configurable True

Platforms Supported on all platforms

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.

Context [system tls generate-self-signed](#)

Tree [generate-self-signed](#)

Configurable True

Platforms Supported on all platforms

common-name *string*

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.

Context [system tls generate-self-signed common-name *string*](#)

Tree [common-name](#)

String Length 1 to 64

Configurable True

Platforms Supported on all platforms

country *string*

Description The country name to use for the certificate signing request
The expected format is two characters long, e.g. 'US'.

Context [system tls generate-self-signed country *string*](#)

Tree [country](#)

String Length 2

Default US

Configurable True

Platforms Supported on all platforms

duration *number*

Description	The time in which the certificate is valid
Context	system tls generate-self-signed duration number
Tree	duration
Range	1 to 3650
Default	365
Units	days
Configurable	True
Platforms	Supported on all platforms

email *string*

Description	The email address to use for the certificate signing request
Context	system tls generate-self-signed email string
Tree	email
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

locality *string*

Description	The city or locality to use for the certificate signing request
Context	system tls generate-self-signed locality string
Tree	locality
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

organization *string*

Description	The organization to use for the certificate signing request
Context	system tls generate-self-signed organization string
Tree	organization
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

organization-unit *string*

Description	The organization unit to use for the certificate signing request
Context	system tls generate-self-signed organization-unit <i>string</i>
Tree	organization-unit
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

state *string*

Description	The state or province to use for the certificate signing request
Context	system tls generate-self-signed state <i>string</i>
Tree	state
String Length	1 to 255
Configurable	True
Platforms	Supported on all platforms

17 tools tunnel

```
tunnel
+ vxlan-tunnel
+   statistics
+     clear
+ vtep address (ipv4-address | ipv6-address)
+   statistics
+     clear
```

17.1 tunnel Descriptions

tunnel

Description	This model collects all config and state aspects of the tools-tunnel table in SR Linux.
Context	tunnel
Tree	tunnel
Configurable	True
Platforms	Supported on all platforms

vxlan-tunnel

Description	Enter the vxlan-tunnel context
Context	tunnel vxlan-tunnel
Tree	vxlan-tunnel
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	tunnel vxlan-tunnel statistics
Tree	statistics
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

clear

Description	Enter the clear context
Context	tunnel vxlan-tunnel statistics clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	tunnel vxlan-tunnel vtep address (<i>ipv4-address</i> <i>ipv6-address</i>)
Tree	vtep
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	tunnel vxlan-tunnel vtep address (<i>ipv4-address</i> <i>ipv6-address</i>)
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	tunnel vxlan-tunnel vtep address (<i>ipv4-address</i> <i>ipv6-address</i>) statistics
Tree	statistics
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

clear

Description	Enter the clear context
Context	tunnel vxlan-tunnel vtep address (<i>ipv4-address</i> <i>ipv6-address</i>) statistics clear
Tree	clear
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

18 tunnel-interface

```

tunnel-interface name string
+ vlan-interface index number
+ bridge-table
- multicast-destinations
- destination vtep (ipv4-address | ipv6-address) vni number
- destination-index number
- multicast-forwarding keyword
- not-programmed-reason keyword
- statistics
- active-entries number
- failed-entries number
- mac-type type keyword
- active-entries number
- failed-entries number
- total-entries number
- total-entries number
- unicast-destinations
- destination vtep (ipv4-address | ipv6-address) vni number
- destination-index number
- mac-table
- mac address string
- failed-slots number
- last-update string
- not-programmed-reason keyword
- type keyword
- statistics
- active-entries number
- failed-entries number
- mac-type type keyword
- active-entries number
- failed-entries number
- total-entries number
- total-entries number
- es-destination esi string
- destination-index number
- mac-table
- mac address string
- failed-slots number
- last-update string
- not-programmed-reason keyword
- type keyword
- statistics
- active-entries number
- failed-entries number
- mac-type type keyword
- active-entries number
- failed-entries number
- total-entries number
- total-entries number
- vtep address (ipv4-address | ipv6-address) vni number
+ egress
+ inner-ethernet-header
+ source-mac keyword
+ source-ip keyword
+ ingress
+ vni number
- oper-down-reason keyword
- oper-state keyword

```

+ **type** *identityref*

18.1 tunnel-interface Descriptions

tunnel-interface *name string*

Description	In the case where the interface is a logical tunnel interface, the parameters for the tunnel are specified within this subtree. Tunnel interfaces have only a single logical subinterface associated with them.
Context	tunnel-interface name string
Tree	tunnel-interface
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

name *string*

Description	The name of the tunnel-interface. Valid options are: vxlan<N>, N=0..255
Context	tunnel-interface name string
String Length	6 to 8
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vxlan-interface *index number*

Description	The list of vxlan-interfaces.
Context	tunnel-interface name string vxlan-interface index number
Tree	vxlan-interface
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3
Max. Elements	16384

index *number*

Description	The index of the vxlan-tunnel.
Context	tunnel-interface name string vxlan-interface index number
Range	0 to 99999999
Configurable	True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

bridge-table

Description Enable the bridge-table context

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table](#)

Tree [bridge-table](#)

Configurable True

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

multicast-destinations

Description Enter the multicast-destinations context

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table](#) [multicast-destinations](#)

Tree [multicast-destinations](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

destination [vtep](#) ([ipv4-address](#) | [ipv6-address](#)) [vni](#) *number*

Description Enter the destination list instance

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table](#) [multicast-destinations](#) [destination vtep](#) ([ipv4-address](#) | [ipv6-address](#)) [vni](#) *number*

Tree [destination](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

[vtep](#) ([ipv4-address](#) | [ipv6-address](#))

Description The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table](#) [multicast-destinations](#) [destination vtep](#) ([ipv4-address](#) | [ipv6-address](#)) [vni](#) *number*

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vni number

Description	VXLAN Network Identifier of the destination.
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table multicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number
Range	1 to 16777215
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

destination-index number

Description	A system-wide unique identifier of this vxlan destination object (system allocated).
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table multicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number destination-index number
Tree	destination-index
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

multicast-forwarding keyword

Description	The type of multicast data forwarded by this vxlan destination.
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table multicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number multicast-forwarding keyword
Tree	multicast-forwarding
Options	<ul style="list-style-type: none"> • none • BUM • unknown-unicast • broadcast-mcast
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

not-programmed-reason keyword

Description	The reason why the destination is not programmed in the floodlist
--------------------	---

Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table multicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number not-programmed-reason <i>keyword</i>
Tree	not-programmed-reason
Options	<ul style="list-style-type: none"> • no-destination-index • multicast-limit
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

active-entries *number*

Description	The total number of entries that are active on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table statistics active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-entries *number*

Description	The total number of macs, which have not been programmed on at least one slot
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table statistics failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-type *type keyword*

Description	The type of the mac on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table statistics mac-type type keyword
Tree	mac-type
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *keyword*

Description	Enter the type context
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table statistics mac-type type keyword
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

active-entries *number*

Description	The total number of entries of this type on the sub-interface
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table statistics mac-type type keyword active-entries number
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-entries *number*

Description	The total number of macs of this type, which have not been programmed on at least one slot
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table statistics mac-type type <i>keyword</i> failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

total-entries *number*

Description	The total number of macs of this type, active and inactive, on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table statistics mac-type type <i>keyword</i> total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

total-entries *number*

Description	The total number of macs, active and inactive, on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table statistics total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

unicast-destinations

Description	Enter the unicast-destinations context
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations
Tree	unicast-destinations

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

destination vtep (*ipv4-address* | *ipv6-address*) *vni number*

Description	Enter the destination list instance
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) <i>vni number</i>
Tree	destination
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) <i>vni number</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vni number

Description	VXLAN Network Identifier of the destination.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) <i>vni number</i>
Range	1 to 16777215
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

destination-index number

Description	A system-wide unique identifier of this vxlan destination object (system allocated).
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) <i>vni number</i> destination-index <i>number</i>

Tree	destination-index
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-table

Description	Enter the mac-table context
Context	tunnel-interface name string vxlan-interface index number bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number mac-table
Tree	mac-table
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac [address string](#)

Description	MACs learnt on the bridging instance
Context	tunnel-interface name string vxlan-interface index number bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number mac-table mac address string
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

address [string](#)

Description	Enter the address context
Context	tunnel-interface name string vxlan-interface index number bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number mac-table mac address string
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-slots [number](#)

Description	The list of slot IDs corresponding to the linecards that did not successfully program the mac
--------------------	---

Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i> mac-table mac address <i>string</i> failed-slots <i>number</i>
Tree	failed-slots
Range	1 to 8
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

last-update *string*

Description	The date and time of the last update of this mac
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i> mac-table mac address <i>string</i> last-update <i>string</i>
Tree	last-update
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

not-programmed-reason *keyword*

Description	The reason why the mac is not programmed
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i> mac-table mac address <i>string</i> not-programmed-reason <i>keyword</i>
Tree	not-programmed-reason
Options	<ul style="list-style-type: none"> • mac-limit • failed-on-slots • no-destination-index • reserved
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *keyword*

Description	The type of the MAC installed in the fib.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni <i>number</i> mac-table mac address <i>string</i> type <i>keyword</i>

Tree	type
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

active-entries *number*

Description	The total number of entries that are active on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number statistics active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-entries *number*

Description	The total number of macs, which have not been programmed on atleast one slot
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number statistics failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-type *type keyword*

Description	the type of the mac on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number statistics mac-type <i>type keyword</i>
Tree	mac-type
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *keyword*

Description	Enter the type context
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number statistics mac-type <i>type keyword</i>
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

active-entries *number*

Description	The total number of entries of this type on the sub-interface
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number statistics mac-type type <i>keyword</i> active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-entries *number*

Description	The total number of macs of this type, which have not been programmed on atleast one slot
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number statistics mac-type type <i>keyword</i> failed-entries <i>number</i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

total-entries *number*

Description	The total number of macs of this type , active and inactive, on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (ipv4-address ipv6-address) vni number statistics mac-type type <i>keyword</i> total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

total-entries *number*

Description	The total number of macs, active and inactive, on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations destination vtep (<i>ipv4-address</i> <i>ipv6-address</i>) vni number statistics total-entries <i>number</i>
Tree	total-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

es-destination *esi string*

Description	Enter the es-destination list instance
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations es-destination esi <i>string</i>
Tree	es-destination
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

esi *string*

Description	The 10-byte Ethernet Segment Identifier of the ethernet segment. ESI-0 or MAX-ESI values are not allowed.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations es-destination esi <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

destination-index *number*

Description	A system-wide unique identifier of this vxlan destination object (system allocated).
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations es-destination esi <i>string</i> destination-index <i>number</i>
Tree	destination-index
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-table

Description	Enter the mac-table context
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> mac-table
Tree	mac-table
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac address *string*

Description	MACs learnt on the bridging instance
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> mac-table mac address <i>string</i>
Tree	mac
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

address *string*

Description	Enter the address context
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> mac-table mac address <i>string</i>
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-slots *number*

Description	The list of slot IDs corresponding to the linecards that did not successfully program the MAC
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> mac-table mac address <i>string</i> failed-slots <i>number</i>
Tree	failed-slots
Range	1 to 8
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

last-update *string*

Description	The date and time of the last update of this MAC
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations es-destination esi <i>string</i> mac-table mac address <i>string</i> last-update <i>string</i>
Tree	last-update
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

not-programmed-reason *keyword*

Description	The reason why the MAC is not programmed
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations es-destination esi <i>string</i> mac-table mac address <i>string</i> not-programmed-reason <i>keyword</i>
Tree	not-programmed-reason
Options	<ul style="list-style-type: none"> • mac-limit • failed-on-slots • no-destination-index • reserved
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *keyword*

Description	The type of MAC installed in the fib.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> bridge-table unicast-destinations es-destination esi <i>string</i> mac-table mac address <i>string</i> type <i>keyword</i>
Tree	type
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast

- proxy-anti-spoof
- reserved
- eth-cfm
- roe

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Enter the statistics context
Context	tunnel-interface name <i>string</i> vxlan-interface index number <i>bridge-table unicast-destinations es-destination esi <i>string</i> statistics</i>
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

active-entries *number*

Description	The total number of entries that are active on the sub-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index number <i>bridge-table unicast-destinations es-destination esi <i>string</i> statistics active-entries <i>number</i></i>
Tree	active-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-entries *number*

Description	The total number of MACs, which have not been programmed on at least one slot
Context	tunnel-interface name <i>string</i> vxlan-interface index number <i>bridge-table unicast-destinations es-destination esi <i>string</i> statistics failed-entries <i>number</i></i>
Tree	failed-entries
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

mac-type *type keyword*

Description	The type of MAC on the sub-interface
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> statistics mac-type type <i>keyword</i>
Tree	mac-type
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *keyword*

Description	Enter the type context
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> statistics mac-type type <i>keyword</i>
Options	<ul style="list-style-type: none"> • static • duplicate • learnt • irb-interface • evpn • evpn-static • irb-interface-anycast • proxy-anti-spoof • reserved • eth-cfm • roe
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

active-entries *number*

Description	The total number of entries of this type on the sub-interface
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> statistics mac-type type <i>keyword</i> active-entries <i>number</i>
Tree	active-entries
Default	0
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

failed-entries *number*

Description The total number of MACs of this type, which have not been programmed on at least one slot

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table unicast-destinations es-destination esi](#) *string* [statistics mac-type type keyword failed-entries](#) *number*

Tree [failed-entries](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

total-entries *number*

Description The total number of MACs of this type, active and inactive, on the sub-interface.

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table unicast-destinations es-destination esi](#) *string* [statistics mac-type type keyword total-entries](#) *number*

Tree [total-entries](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

total-entries *number*

Description The total number of MACs, active and inactive, on the sub-interface.

Context [tunnel-interface name](#) *string* [vxlan-interface index](#) *number* [bridge-table unicast-destinations es-destination esi](#) *string* [statistics total-entries](#) *number*

Tree [total-entries](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vtep [address](#) (*ipv4-address* | *ipv6-address*) [vni](#) *number*

Description Add a list entry for VTEP

Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> vtep address (ipv4-address ipv6-address) vni number
Tree	vtep
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

address (ipv4-address | ipv6-address)

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> vtep address (ipv4-address ipv6-address) vni number
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vni number

Description	VXLAN Network Identifier of the destination.
Context	tunnel-interface name <i>string</i> vxlan-interface index number bridge-table unicast-destinations es-destination esi <i>string</i> vtep address (ipv4-address ipv6-address) vni number
Range	1 to 16777215
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

egress

Description	Enter the egress context
Context	tunnel-interface name <i>string</i> vxlan-interface index number egress
Tree	egress
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

inner-ethernet-header

Description	Parameters of the inner VXLAN ethernet payload when the VXLAN tunnel is used in an ip-vrf.
--------------------	--

Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> egress inner-ethernet-header
Tree	inner-ethernet-header
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

source-mac *keyword*

Description	VXLAN inner ethernet source mac-address. Present when the VXLAN tunnel is associated with a ip-vrf network-instance.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> egress inner-ethernet-header source-mac <i>keyword</i>
Tree	source-mac
Default	use-system-mac
Options	<ul style="list-style-type: none"> • use-system-mac
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

source-ip *keyword*

Description	The ip-address that will be used as the source-ip for all vxlan traffic egressing this vxlan-interface.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> egress source-ip <i>keyword</i>
Tree	source-ip
Default	use-system-ipv4-address
Options	<ul style="list-style-type: none"> • use-system-ipv4-address
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

ingress

Description	Enter the ingress context
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> ingress
Tree	ingress
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vni number

Description	Ingress VXLAN Network Identifier of the VXLAN subinterface. The egress VNI is determined by the static egress-vni configured in the associated destination or by the dynamic egress-vni learned from the control plane.
Context	tunnel-interface name <i>string</i> vxlan-interface index number ingress vni number
Tree	vni
Range	1 to 16777215
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-down-reason keyword

Description	The reason why the vxlan-interface is oper-down
Context	tunnel-interface name <i>string</i> vxlan-interface index number oper-down-reason keyword
Tree	oper-down-reason
Options	<ul style="list-style-type: none"> • mac-failed • ingress-hash-failed • egress-hash-failed • other
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

oper-state keyword

Description	The operational state of the vxlan-interface
Context	tunnel-interface name <i>string</i> vxlan-interface index number oper-state keyword
Tree	oper-state
Options	<ul style="list-style-type: none"> • up • down
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

type *identityref*

Description	The value of this leaf indicates the context in which the vxlan-interface will be used in.
Context	tunnel-interface name <i>string</i> vxlan-interface index <i>number</i> type identityref
Tree	type
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• local-mirror-dest indicates subinterface is used in a mirroring destination SPAN context
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

19 tunnel

```
tunnel
+ vxlan-tunnel
- statistics
  - in-discarded-packets number
  - in-octets number
  - in-packets number
  - last-clear string
  - out-octets number
  - out-packets number
- vtep address (ipv4-address | ipv6-address)
  - index number
  - last-change string
  - statistics
    - in-discarded-packets number
    - in-octets number
    - in-packets number
    - last-clear string
    - out-discarded-packets number
    - out-octets number
    - out-packets number
```

19.1 tunnel Descriptions

tunnel

Description	This model collects all config and state aspects of the tunnel table in SR Linux.
Context	tunnel
Tree	tunnel
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

vxlan-tunnel

Description	Enter the vxlan-tunnel context
Context	tunnel vxlan-tunnel
Tree	vxlan-tunnel
Configurable	True
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description	Container for vxlan-tunnel global statistics.
Context	tunnel vxlan-tunnel statistics
Tree	statistics
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

in-discarded-packets *number*

Description	The total number of discarded ingress VXLAN packets. Ingress VXLAN packets can be discarded due to one of the following reasons:
Context	tunnel vxlan-tunnel statistics in-discarded-packets number
Tree	in-discarded-packets
Default	0
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

in-octets *number*

Description The total sum of ingress VXLAN octets.
Context [tunnel vxlan-tunnel statistics in-octets number](#)
Tree [in-octets](#)
Default 0
Configurable False
Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

in-packets *number*

Description The total sum of ingress VXLAN packets.
 A packet in this context is an inner frame.
Context [tunnel vxlan-tunnel statistics in-packets number](#)
Tree [in-packets](#)
Default 0
Configurable False
Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

last-clear *string*

Description Timestamp of the last time the vxlan tunnel counters were cleared.
Context [tunnel vxlan-tunnel statistics last-clear string](#)
Tree [last-clear](#)
String Length 20 to 32
Configurable False
Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

out-octets *number*

Description The total sum of egress VXLAN octets
Context [tunnel vxlan-tunnel statistics out-octets number](#)
Tree [out-octets](#)
Default 0

Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

out-packets *number*

Description	The total sum of egress VXLAN packets. . A packet in this context is an inner frame.
Context	tunnel vxlan-tunnel statistics out-packets number
Tree	out-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address)
Tree	vtep
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

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

Description	The IP address that identifies the remote VXLAN Termination Endpoint (VTEP).
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address)
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

index *number*

Description	The next-hop-group-id (system allocated) for resolving the VXLAN termination endpoint
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address) index number
Tree	index
Configurable	False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

last-change *string*

Description The date and time of the most recent change to the tunnel state

Context [tunnel vxlan-tunnel vtep address \(ipv4-address | ipv6-address\)](#) [last-change string](#)

Tree [last-change](#)

String Length 20 to 32

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

statistics

Description Container for vxlan-tunnel per VTEP (Vxlan Termination EndPoint) statistics.

Context [tunnel vxlan-tunnel vtep address \(ipv4-address | ipv6-address\)](#) [statistics](#)

Tree [statistics](#)

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

in-discarded-packets *number*

Description The number of discarded ingress VXLAN packets.
Ingress VXLAN packets can be discarded due to one of the following reasons:

Context [tunnel vxlan-tunnel vtep address \(ipv4-address | ipv6-address\)](#) [statistics in-discarded-packets](#) [number](#)

Tree [in-discarded-packets](#)

Default 0

Configurable False

Platforms 7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

in-octets *number*

Description The number of octets encapsulated in ingress VXLAN packets.

Context [tunnel vxlan-tunnel vtep address \(ipv4-address | ipv6-address\)](#) [statistics in-octets](#) [number](#)

Tree [in-octets](#)

Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

in-packets *number*

Description	The number of packets encapsulated in ingress VXLAN packets. A packet in this context is an inner frame.
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address) statistics in-packets number
Tree	in-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

last-clear *string*

Description	Timestamp of the last time the vxlan tunnel counters were cleared.
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address) statistics last-clear string
Tree	last-clear
String Length	20 to 32
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

out-discarded-packets *number*

Description	The number of discarded egress VXLAN packets. Egress VXLAN packets can be discarded due to one of the following reasons:
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address) statistics out-discarded-packets number
Tree	out-discarded-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

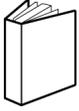
out-octets *number*

Description	The number of octets encapsulated in egress VXLAN packets.
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address) statistics out-octets number
Tree	out-octets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

out-packets *number*

Description	The number of packets encapsulated in egress VXLAN packets. A packet in this context is an inner frame.
Context	tunnel vxlan-tunnel vtep address (ipv4-address ipv6-address) statistics out-packets number
Tree	out-packets
Default	0
Configurable	False
Platforms	7220 IXR-D2L, 7220 IXR-D2, 7220 IXR-D3L, 7220 IXR-D3

Customer document and product support



Customer documentation

[Customer documentation welcome page](#)



Technical support

[Product support portal](#)



Documentation feedback

[Customer documentation feedback](#)