IP Addresses and Services Command Reference for Cisco 8000 Series Routers

First Published: 2020-03-01

Last Modified: 2024-09-04

Americas Headquarters

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

CONTENTS

PREFACE

CHAPTER 1

Preface

This preface contains these sections:

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

Date	Summary
September 2024	Republished for Cisco IOS XR Release 24.3.1.
March 2024	Republished for Cisco IOS XR Release 24.1.1.
August 2023	Republished for Cisco IOS XR Release 7.10.1.
May 2021	Republished for Cisco IOS XR Release 7.3.15.
February 2021	Republished for Cisco IOS XR Release 7.3.1.
October 2020	Republished for Cisco IOS XR Release 7.2.12.
March 2020	Initial release of this document.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Access List Commands

This module describes the Cisco IOS XR software commands used to configure IP Version 4 (IPv4) and IP Version 6 (IPv6) access lists.

For detailed information about ACL concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

clear access-list ipv4

To clear IPv4 access list counters, use the **clear access-list ipv4** command in XR EXEC mode.

clear access-list ipv4 *access-list-name* **hardware** {**clear access-list ipv4** *access-list-name* **hardware** {**ingress** | **egress** } [**interface** *interface-path-id*] [**sequence** *sequence-number*] [**location** *node-id*]}

Syntax Description

access-list-name	Name of a particular IPv4 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
sequence-number	(Optional) Specific sequence number with which counters are cleared for an access list. Range is 1 to 2147483644.
ingress	Specifies an inbound direction.
egress	Specifies an outbound direction.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Clears hardware resource counters from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The default clears the specified IPv4 access list.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **clear access-list ipv4** command to clear counters for a specified configured access list. Use a sequence number to clear counters for an access list with a specific sequence number.

Use an asterisk (***)** in place of the *access-list-name* argument to clear all access lists.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write
bgp	read, write, execute

Examples

In the following example, counters for an access list named *marketing* are cleared:

```
Router# show access-lists ipv4 marketing hardware ingress location 0/RP0/CPU0
ipv4 access-list marketing
10 permit ipv4 192.168.34.0 0.0.0.255 any
20 permit ipv4 172.16.0.0 0.0.255.255 any
30 deny tcp host 172.16.0.0 eq 2330 host 192.168.202.203 (23345 matches)

Router# clear access-list ipv4 marketing hardware ingress location 0/RP0/CPU0
```

clear access-list ipv6

To clear IPv6 access list counters, use the **clear access-list ipv6** command in .

clear access-list ipv4 *access-list-name* **hardware** {**ingress** | **egress** } [**interface** *interface-path-id*] [**sequence** *sequence-number*] [**location** *node-id*]

Syntax Description

access-list-name	Name of a particular IPv6 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
sequence-number	(Optional) Specific sequence number for a particular access control entry (ACE) with which counters are cleared for an access list. Range is 1 to 2147483644.
ingress	(Optional) Specifies an inbound direction.
egress	(Optional) Specifies an outbound direction.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Clears counters for an access list enabled on a card interface. The *node-id* argument is entered in the rack/slot/module notation.

Command Default

The default clears the specified IPv6 access list.

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **clear access-list ipv6** command is similar to the **clear access-list ipv4** command, except that it is IPv6-specific.

Use the **clear access-list ipv6** command to clear counters for a specified configured access list. Use a sequence number to clear counters for an access list with a specific sequence number

Use an asterisk (*****) in place of the *access-list-name* argument to clear all access lists.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write

Task ID	Operations
network	read, write

Examples

In the following example, counters for an access list named *marketing* are cleared:

```
Router# show access-lists ipv6 marketing hardware ingress location 0/RP0/CPU0
ipv6 access-list marketing
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
Router# clear access-list ipv6 marketing hardware ingress location 0/RP0/CPU0
```

copy access-list ipv4

To create a copy of an existing IPv4 access list, use the **copy access-list ipv4** command in XR EXEC mode.

copy access-list ipv4 *source-acl destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Name of the destination access list where the contents of the *source-acl* argument is copied.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **copy access-list ipv4** command to copy a configured access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name exists for an access list or prefix list, the access list is not copied. The **copy access-list ipv4** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In the following example, a copy of access list list-1 is created:

```
Router# show access-lists ipv4 list-1

ipv4 access-list list-1
  10 permit tcp any any log
  20 permit ip any any
Router# copy access-list ipv4 list-1 list-2
Router# show access-lists ipv4 list-2
ipv4 access-list list-2
  10 permit tcp any any log
  20 permit ip any any
```

In the following example, copying the access list list-1 to list-3 is denied because a list-3 access list already exists:

```
Router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list

Router# show access-lists ipv4 list-3

ipv4 access-list list-3
  10 permit ip any any
  20 deny tcp any any log
```

copy access-list ipv6

To create a copy of an existing IPv6 access list, use the **copy access-list ipv6** command in .

copy **access-list** **ipv6** *source-acl* *destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Destination access list where the contents of the *source-acl* argument is copied.

Command Default

No default behavior or value

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **copy access-list ipv6** command to copy a configured access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name exists for an access list or prefix list, the access list is not copied. The **copy access-list ipv6** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In this example, a copy of access list list-1 is created:

```
Router# show access-lists ipv6 list-1

ipv6 access-list list-1
  10 permit tcp any any log
  20 permit ipv6 any any

Router# copy access-list ipv6 list-1 list-2

Router# show access-lists ipv6 list-2

ipv6 access-list list-2
  10 permit tcp any any log
  20 permit ipv6 any any
```

In this example, copying access list list-1 to list-3 is denied because a list-3 access list already exists:

```
Router# copy access-list ipv6 list-1 list-3

list-3 exists in access-list

Router# show access-lists ipv6 list-3
ipv6 access-list list-3
  10 permit ipv6 any any
  20 deny tcp any any log
```

deny (IPv4)

To set conditions for an IPv4 access list, use the **deny** command in access list configuration mode. There are two versions of the **deny** command: **deny** (source), **deny** (destination), and **deny** (protocol). To remove a condition from an access list, use the **no** form of this command.

[*sequence-number*] **deny** *source* [*source-wildcard*] [**log** | | **log-input**]
[*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**dscp** *dscp* [**bitmask** *value*]] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**]
no *sequence-number*

Internet Control Message Protocol (ICMP)
[*sequence-number*] **deny icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log**][**icmp-off**]

Transmission Control Protocol (TCP)
[sequence-number] **permit tcp** { *source-ipv4-prefix/ prefix-length* | *any* | *host source-ipv4-address ipv4-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol-port* }] { *destination-ipv4-prefix/ prefix-length* | *any* | *host destination-ipv4-address ipv4-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol* | *port* }] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] { **match-any | match-all | + | -** } [*flag-name*] [**log**]

Internet Group Management Protocol (IGMP)
[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] [**fragments**] [**log**]

User Datagram Protocol (UDP)
[*sequence-number*] **deny udp** *source source-wildcard* [*operator* {*portprotocol-port*}] *destination destination-wildcard* [*operator* {*portprotocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log**]

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an IP protocol. It can be one of the keywords **ahp** , **esp** , **gre** , **icmp** , **igmp** , **igrp** , **ip** , **ipinip** , **nos** , **ospf** , **pim** , **pcp** , **tcp** , or **udp** , or an integer from 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. ICMP, and TCP allow further qualifiers, which are described later in this table. **Note** Filtering on AHP protocol is not supported.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names: • **routine** —Match packets with routine precedence (0) • **priority** —Match packets with priority precedence (1) • **immediate** —Match packets with immediate precedence (2) • **flash** —Match packets with flash precedence (3) • **flash-override** —Match packets with flash override precedence (4) • **critical** —Match packets with critical precedence (5) • **internet** —Match packets with internetwork control precedence (6) • **network** —Match packets with network control precedence (7)

dscp *dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • **0**–**63**–Differentiated services codepoint value • **af11**—Match packets with AF11 dscp (001010) • **af12**—Match packets with AF12 dscp (001100) • **af13**—Match packets with AF13 dscp (001110) • **af21**—Match packets with AF21 dscp (010010) • **af22**—Match packets with AF22 dscp (010100) • **af23**—Match packets with AF23 dscp (010110) • **af31**—Match packets with AF31 dscp (011010) • **af32**—Match packets with AF32 dscp (011100) • **af33**—Match packets with AF33 dscp (011110) • **af41**—Match packets with AF41 dscp (100010) • **af42**—Match packets with AF42 dscp (100100) • **af43**—Match packets with AF43 dscp (100110) • **cs1**—Match packets with CS1 (precedence 1) dscp (001000) • **cs2**—Match packets with CS2 (precedence 2) dscp (010000) • **cs3**—Match packets with CS3 (precedence 3) dscp (011000) • **cs4**—Match packets with CS4 (precedence 4) dscp (100000) • **cs5**—Match packets with CS5 (precedence 5) dscp (101000) • **cs6**—Match packets with CS6 (precedence 6) dscp (110000) • **cs7**—Match packets with CS7 (precedence 7) dscp (111000) • **default**—Default DSCP (000000) • **ef**—Match packets with EF dscp (101110)
fragments	(Optional) Causes the software to examine fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) **Note** ACL logging is supported only in ingress direction for both IPv4 and IPv6. The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches a flow, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
icmp-off	(Optional) Turns off ICMP generation for denied packets.
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.

icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.
igmp-type	(Optional) IGMP message type (0 to 15) or message name for filtering IGMP packets, as follows: • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report
operator	(Optional) Operator is used to compare source or destination ports. Possible operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* values, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* values, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	Decimal number of a TCP or UDP port. A port number is a number from 0 to 65535. TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.
protocol-port	Name of a TCP or UDP port. TCP and UDP port names are listed in the "Usage Guidelines" section. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with **+** or **-** . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack** , **fin** , **psh** , **rst** , **syn** , **urg**.

Command Default

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.8.1	**log-input** keyword was introduced.
Release 7.5.4	**bitmask** keyword was introduced.

Usage Guidelines

Use the **deny** command following the **ipv4 access-list** command to specify conditions under which a packet cannot pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

The following is a list of precedence names:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The following is a list of ICMP message type names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable

- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- unreachable

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident

- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The following UDP port names can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time

- who
- xdmcp

Use the following flags in conjunction with the **match-any** and **match-all** keywords and the + and - signs to select the flags to display:

- ack
- fin
- psh
- rst
- syn

For example, **match-all** + *ack* + *syn* displays TCP packets with both the ack *and* syn flags set, or **match-any** + *ack* - *syn* displays the TCP packets with the ack set *or* the syn not set.

Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

This example shows how to set a deny condition for an access list named Internet filter:

```
Router(config)# ipv4 access-list Internetfilter
Router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
Router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
Router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 gt bgp host 192.168.202.203 range 1300
 1400
Router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

This example shows how you can configure DSCP bitmask on ingress ERSPAN.

```
Router# config
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit
Router(config)# interface HundredGigE0/0/0/6
Router(config-if)# ipv4 address 192.0.2.51 255.255.255.0
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv4 acl1
Router(config-if)# commit
```

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

[sequence-number] **deny** *protocol* { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/ prefix-length* } [*operator* { *port* | *protocol-port* }] [**dscp** *value* [**bitmask** *value*]] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log | log-input**] [**ttl** *ttl value* [*value1* **. . .** *value2*]] **icmp-off**]
no *sequence-number*

Internet Control Message Protocol (ICMP)
[sequence-number] **deny icmp** { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/ prefix-length* } { *destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/ prefix-length* } [*icmp-type*] [*icmp-code*] [**dscp** *value*] [routing] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**log**] [**icmp-off**]

Transmission Control Protocol (TCP)
*[sequence-number]***deny tcp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/ prefix-length*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/ prefix-length*} [*operator* {*port* | *protocol* | *port*}] [**dscp***value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] {**match-any | match-all | + | -**} [*flag-name*] [**log**] [**icmp-off**]

User Datagram Protocol (UDP)
*[sequence-number]***deny tcp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/ prefix-length*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/ prefix-length*} [*operator* {*port* | *protocol* | *port*}] [**dscp***value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] [*flag-name*] [**log**] [**icmp-off**]

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp** , **esp** , **gre**, **icmp** , **igmp**, **igrp**, **ipinip**, **ipv6** , **nos**, **ospf**, **pcp** , **tcp** , or **udp** , or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix / *prefix-length*	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	Source IPv6 host address about which to set deny conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

ipv6-wildcard-mask	IPv6 wildcard mask. The IPv6 wildcard mask can take any IPv6 address value which is used instead of prefix length.
operator {*port* | *protocol-port*}	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix / prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix / prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The *port* argument is the decimal number of a TCP or UDP port. Range is 0 to 65535. The *protocol-port* argument is the name of a TCP or UDP port. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix / *prefix-length*	Destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	Destination IPv6 host address about which to set deny conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dscp *value*	(Optional) Matches a differentiated services code point DSCP value against the traffic class value in the Traffic Class field of each IPv6 packet header. Range is 0 to 63.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
hop-by-hop	(Optional) Supports Jumbo-grams. With the Router Alert option, it is an integral part in the operation of Multicast Listener Discovery (MLD). Router Alert [3] is an integral part in the operations of IPv6 Multicast through MLD and RSVP for IPv6.
authen	(Optional) Matches if the IPv6 egress authentication header is present.
destopts	(Optional) Matches if the IPv6 egress destination options header is present.
fragments	(Optional) Matches noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) **Note** ACL logging is supported only in ingress direction for both IPv4 and IPv6. The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value. For IPv6 packets, **ttl** is also referred to as hop limit.
ttl value [*value1 ... value2*]	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
operator	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
icmp-off	(Optional) Turns off ICMP generation for denied packets.
icmp-type	(Optional) ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. Range is 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. Range is 0 to 255.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with **+** or **-** . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack**, **fin**, **psh**, **rst**, **syn**, **urg**.

Command Default

ICMP message generation is enabled by default.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.2.1	Ingress IPv6 TCP flags are supported.
Release 7.3.15	Egress IPv6 TCP flags are supported.
Release 7.8.1	**log-input** keyword was introduced.
Release 7.8.1	**ttl** keyword was introduced.
Release 7.5.4	**bitmask** keyword was introduced.
Release 7.10.1	IPv6 AHP and ESP headers are supported.

Usage Guidelines

The **deny** (IPv6) command is similar to the **deny** (IPv4) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list.

Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

Specifying **ipv6** for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add permit, deny, or remark statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port* | *protocol-port*] arguments are not specified.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to configure the IPv6 access list named toCISCO and apply the access list to the traffic entering the HundredGigE interface 0/2/0/2. Specifically, the deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from entering the HundredGigE interface 0/2/0/2. The permit entry in the list permits all ICMP packets to enter the HundredGigE interface 0/2/0/2.

```
Router(config)# ipv6 access-list toCISCO
Router(config-ipv6-acl)# deny tcp any any gt 5000
Router(config-ipv6-acl)# permit icmp any any
Router(config)#  interface HundredGigE 0/2/0/2
Router(config-if)# ipv6 access-group tOCISCO ingress
```

The following example shows how to configure the IPv6 access list named toCISCO and apply the access list to the traffic entering theHundredGigE interface 0/2/0/2. Specifically, the deny entry in the list keeps all packets that have a hop-by-hop optional field from entering the HundredGigE interface 0/2/0/2.

```
Router(config)# ipv6 access-list toCISCO
Router(config-ipv6-acl)# deny ipv6 any any hop-by-hop
Router(config)#  interface HundredGigE 0/2/0/2
Router(config-if)# ipv6 access-group tOCISCO ingress
```

The following example shows how you can configure DSCP bitmask on ingress ERSPAN.

```
Router# config
Router(config)# ipv6 access-list acl1
Router(config-ipv6-acl)# 10 permit ipv6 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
Router(config)# interface HundredGigE 0/0/10/3
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
Router(config-if)# commit
```

The following example shows how you can configure AHP and ESP headers on an ACLs.

```
Router(config)# #ipv6 access-list ipv6_umpp_access_list
Router(config-ipv6-acl)# 12 deny ahp any any
Router(config-ipv6-acl)# ipv6 access-list ipv6_umpp_access_list
Router(config-ipv6-acl)# 14 deny esp any any
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
```

dont-fragment

To configure an access list to match on the **dont-fragment** flag.

fragment-type dont-fragment {**capture** | **counter** | **first-fragment** | **is-fragment** | **last-fragment** | **log** | **log-input** | **set** | **udf** | **nexthop1** }

Syntax Description

capture	ACL matches on the **dont-fragment** flag, and captures the matched packet.
counter	ACL matches on the **dont-fragment** flag, and displays the counter for the matches.
first-fragment	ACL matches on the **dont-fragment** flag, and then matches on the **first-fragment** flag.
is-fragment	ACL matches on the **dont-fragment** flag, and then matches on the **is-fragment** flag.
last-fragment	ACL matches on the **dont-fragment** flag, and then matches on the **last-fragment** flag.
log	ACL matches on the **dont-fragment** flag and logs the matches.
log-input	ACL matches on the **dont-fragment** flag and logs the matches, incuding on the input interface.
set	ACL matches on the **dont-fragment** flag and sets a particular action on the matches.
udf	ACL matches on the **dont-fragment** flag, and sets the user-defined fields for the matches.
nexthop1	ACL matches on the **dont-fragment** flag, and then matches on the **nexthop1** flag.

Command Default

None

Command Modes

ACL configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

This command is supported only for IPv4 ACLs.

Example

Use the following sample configuration to match on the **dont-fragment** flag.

```
/* Enter the global configuraton mode and configure an IPv4 access list */
Router# config
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit tcp any any

/* Configure an ACE to match on the dont-fragment flag (indicates a non-fragmented packet)
 and forward the packet to the default (pre-configured) next hop  */
Router(config-ipv4-acl)# 20 permit tcp any any fragment-type dont-fragment nexthop1 ipv4
```

```
192.0.2.1
Router(config-ipv4-acl)# commit
```

first-fragment

To configure an ACL to match on the **first-fragment** flag.

fragment-type first-fragment {**capture** | **counter** | **log** | **log-input** | **set** | **udf** | **<none>**}

Syntax Description

capture	ACL matches on the **first-fragment** flag, and captures the matched packet.
counter	ACL matches on the **first-fragment** flag, and displays the counter for the matches.
log	ACL matches on the **first-fragment** flag and logs the matches.
log-input	ACL matches on the **first-fragment** flag and logs the matches, incuding on the input interface.
set	ACL matches on the **first-fragment** flag and sets a particular action on the matches.
udf	ACL matches on the **first-fragment** flag, and sets the user-defined fields for the matches.
nexthop1	ACL matches on the **first-fragment** flag, and then matches on the **nexthop1** flag.

Command Default

None

Command Modes

ACL configuration mode.

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

This command is supported only for IPv4 ACLs.

Example

Use the following sample configuration to match on the **first-fragment** flag.

```
/* Enter the global configuraton mode and configure an IPv4 access list */
Router# config
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit tcp any any

/* Configure an ACE to match on the first-fragment flag (indicates the first fragment of a
 fragmented packet)
 and forward the packet to a next hop of 20.20.20.1  */
Router(config-ipv4-acl)# 40 permit ospf any any fragment-type first-fragment nexthop1 ipv4
 192.0.2.1
Router(config-ipv4-acl)# commit
```

fragment-offset

To enable packet filtering at an ingress or egress interface by specifying fragment-offset as a match condition in an IPv4 or IPv6 ACL, use the **fragment-offset** option in **permit** or **deny** command in IPv4 or IPv6 access-list configuration mode. To disable this feature, use the **no** form of this command.

fragment-offset {**eq** *value* | **gt** *value* | **lt** *value* | **neq** *value* | **range** *lower-limit* *upper-limit*}

Syntax Description

fragment-offset eq *value*	Filters packets that have a fragment offset equal to the specified limit.
fragment-offset gt *value*	Filters packets that have a fragment offset greater than the specified limit.
fragment-offset lt *value*	Filters packets that have a fragment offset less than the specified limit.
fragment-offset neq *value*	Filters packets that have a fragment offset that does not match the specified limit.
fragment-offset range *lower-limit upper-limit*	Filters packets that have a fragment offset within the specified range.

Command Default

None

Command Modes

IPv4 or IPv6 Access List Configuration mode

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

This example shows how to configure an IPv4 access list to filter packets by the fragment-offset condition:

```
Router# config
Router(config)# ipv4 access-list fragment-offset-acl
Router(config-ipv4-acl)# 10 permit ipv4 any any fragment-offset range 300 400
```

fragment-type

To configure an access list to match on the type of fragment.

fragment-type {**dont-fragment** | **first-fragment** | **is-fragment** | **last-fragment**}

Syntax Description

dont-fragment	ACL matches on the **dont-fragment** flag
first-fragment	ACL matches on the **first-fragment** flag
is-fragment	ACL matches on the **is-fragment** flag
last-fragment	ACL matches on the **last-fragment** flag

Command Default

None

Command Modes

ACL configuration mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

This command is supported only for IPv4 access lists.

Example

Use the following sample configuration to configure an ACL to match on the type of fragment..

```
/* Enter the global configuraton mode and configure an IPv4 access list */
Router# config
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit tcp any any

/* Configure an ACE to match on the dont-fragment flag (indicates a non-fragmented packet)
 and forward the packet to the default (pre-configured) next hop  */
Router(config-ipv4-acl)# 20 permit tcp any any fragment-type dont-fragment default

/* Configure an ACE to match on the is-fragment flag (indicates a fragmented packet)
 and forward the packet to a next hop of 10.10.10.1  */
Router(config-ipv4-acl)# 30 permit udp any any fragment-type is-fragment nexthop1 ipv4
10.10.10.1

/* Configure an ACE to match on the first-fragment flag (indicates the first fragment of a
 fragmented packet)
 and forward the packet to a next hop of 20.20.20.1  */
Router(config-ipv4-acl)# 40 permit ospf any any fragment-type first-fragment nexthop1 ipv4
 20.20.20.1


/* Configure an ACE to match on the last-fragment flag (indicates the last fragment of a
fragmented packet)
 and forward the packet to a next hop of 30.30.30.1  */
```

```
Router(config-ipv4-acl)# 50 permit icmp any any fragment-type last-fragment nexthop1 ipv4
30.30.30.1
Router(config-ipv4-acl)# commit
```

hw-module profile stats acl-permit

To obtain statistics of the packet count of the routing traffic that an ACL permits, use the **hw-module profile stats acl-permit** command in XR Config mode. To disable the tracking of permitted packet count, use the **no** form of this command.

hw-module profile stats acl-permit
no hw-module profile stats acl-permit

Syntax Description

This command has no keywords or arguments.

Command Default

If you do not configure the **hw-module profile stats acl-permit** command, you cannot enable the statistics for the routing traffic that an ACL permits.

Command Mode

XR Config

Command History

Release	Modification
Release 7.3.2	Supports logging of permit statistics for ACL-based forwarding (ABF).
Release 7.2.12	This command was introduced.

Usage Guidelines

- The permit statistics of the routing traffic that an ACL allows are available only after you execute the **hw-module profile stats acl-permit** command and based on the requirement, reboot the line cards or the router.

Task ID	Operations
config-services	read, write
root-lr	read, write

Examples

The following example shows you how to configure the **acl-permit** command:

```
Router# configure
Router(config)# hw-module profile stats acl-permit
Fri Aug  7 05:52:58.052 UTC
In order to activate/deactivate this stats profile, you must manually reload the chassis/all
 line cards
Router(config)# commit
Fri Aug 7 05:55:50.103 UTC
```

```
LC/0/4/CPU0:Aug 7 05:55:50.218 UTC: fia_driver[245]:
%FABRIC-FIA_DRVR-4-STATS_HW_PROFILE_MISMATCH : Mismatch found, reload LC to activate the
new stats profile
Router(config)#
```

ipv4 access-group

To control access to an interface, use the **ipv4 access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ipv4 access-group *access-list-name* { **ingress** | **egress** } [**compress level** *compression-level*]

Syntax Description

access-list-name	Name of an IPv4 access list as specified by an **ipv6 access-list** command.
ingress	Filters on inbound packets.
egress	Filters on outbound packets.
compress level *compression-level*	Configures compression level for interface ACLs. Compression level values range from zero and five.

Command Default

The interface does not have an IPv4 access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.3.1	Compression level can be configured

Usage Guidelines

Use the **ipv4 access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* argument to specify a particular IPv4 access list.

Filtering of MPLS packets through interface ACL is not supported.

If the access list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified access list does not exist, all packets are passed.

By default, the unique or per-interface ACL statistics are disabled.

Task ID

Task ID	Operations
acl	read, write
network	read, write

Examples

The following example shows how to apply filters on packets from HundredGigE interface 0/2/0/2:

```
Router(config)# interface HundredGigE 0/2/0/2
Router(config-if)# ipv4 access-group p-ingress-filter ingress
```

The following example shows how to apply compress level 2 on ingress traffic:

```
Router(config)# interface HundredGigE 0/2/0/0
Router(config-if)# ipv4 access-group p-ingress-filter ingress compress level 2
```

This example shows how to apply compression level 2 on egress traffic for an IPv4 Hybrid ACL, where you've already created a network object group and attached an ACL(network-object-acl) to it:

```
Router# configure
Router(config)# interface HundredGigE 0/0/10/3
Router(config-if)# ipv4 address 1.1.1.1/24
Router(config-if)# no shut
Router(config-if)# ipv4 access-group network-object-acl egress compress level 2
Router(config-if)# commit
Router(config-if)# exit
```

ipv4 access-list

To define an IPv4 access list by name, use the **ipv4 access-list** command in XR Config mode. To remove all entries in an IPv4 access list, use the **no** form of this command.

ipv4 access-list *name*
no ipv4 access-list *name*

Syntax Description

name	Name of the access list. Names cannot contain a space or quotation marks.

Command Default

No IPv4 access list is defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **ipv4 access-list** command to configure an IPv4 access list. This command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined with the **deny** or **permit** command.

Use the **ipv4 access-group** command to apply the access list to an interface.

Task ID

Task ID	Operations
acl	read, write

Examples

This example shows how to define a standard access list named Internetfilter:

```
Router(config)# ipv4 access-list Internetfilter
Router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
Router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
Router(config-ipv4-acl)# 30 permit 10.0.0.0 0.255.255.255
Router(config-ipv4-acl)# 39 remark Block BGP traffic from 172.16 net.
Router(config-ipv4-acl)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 range 1300
 1400
```

ipv4 access-list log-update rate

To specify the rate at which IPv4 access lists are logged, use the **ipv4 access-list log-update rate** command in XR Config mode. To return the update rate to the default setting, use the **no** form of this command.

ipv4 access-list log-update rate *rate-number*
no ipv4 access-list log-update rate *rate-number*

Syntax Description

rate-number	Rate at which IPv4 access hit logs are generated per second on the router. Range is 1 to 1000.

Command Default

Default is 1.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The *rate-number* argument applies to all the IPv4 access-lists configured on the interfaces. That is, at any given time there can be between 1 and 1000 log entries for the system.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to configure a IPv4 access hit logging rate for the system:

```
Router(config)# ipv4 access-list log-update rate 10
```

ipv4 access-list log-update threshold

To specify the number of updates that are logged for IPv4 access lists, use the **ipv4 access-list log-update threshold** command in XR Config mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv4 access-list log-update threshold *update-number*
no ipv4 access-list log-update threshold *update-number*

Syntax Description

update-number	Number of updates that are logged for every IPv4 access list configured on the router. Range is 0 to 2147483647.

Command Default

For IPv4 access lists, 2147483647 updates are logged.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

IPv4 access list updates are logged at 5-minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write

Examples

This example shows how to configure a log threshold of ten updates for every IPv4 access list configured on the router:

```
Router(config)# ipv4 access-list log-update threshold 10
```

ipv6 access-group

To control access to an interface, use the **ipv6 access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ipv6 access-group *access-list-name* { **ingress** | **egress** } [**compress level** *compression-level*]

Syntax Description

access-list-name	Name of an IPv6 access list as specified by an **ipv6 access-list** command.
ingress	Filters on inbound packets.
compress level *compression-level*	Configures compression level for interface ACLs. Compression level values range from zero and five.

Command Default

The interface does not have an IPv6 access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.3.1	Compression level can be configured

Usage Guidelines

Use compression level two to create Hybrid ACLs with an ACE that uses IPv6 extension headers to filter ingress and egress IPv6 packets.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to apply filters on packets from HundredGigE interface 0/2/0/2:

```
Router(config)# interface HundredGigE 0/2/0/2
Router(config-if)# ipv6 access-group p-in-filter ingress
```

This example shows how to create an ingress IPv6 Hybrid ACL with compression level 2 based on extensions headers:

```
Router# configure
Router(config)# ipv6 access-list ACL-EXT-HEADER
Router(config-ipv6-acl)# 10 deny ipv6 any any routing
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
Router(config)# interface hundredGigE 0/4/0/36
Router(config-if)# ipv6 access-group ACL-EXT-HEADER ingress compress level 2
Router(config-if)# commit
```

This example shows how to create an egress IPv6 Hybrid ACL with compression level 2 based on extensions headers:

```
Router# configure
Router(config)# ipv6 access-list ACL-EGRESS
Router(config-ipv6-acl)# 10 deny ipv6 any any routing
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
Router(config)# interface hundredGigE 0/4/0/13
Router(config-if)# ipv6 access-group ACL-EGRESS egress compress level 2
Router(config-if)# commit
```

ipv6 access-list

To define an IPv6 access list and to place the router in IPv6 access list configuration mode, use the **ipv6 access-list** command in interface configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *name*
no ipv6 access-list *name*

Syntax Description

name	Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No IPv6 access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command is similar to the **ipv4 access-list** command, except that it is IPv6-specific.

The IPv6 access lists are used for traffic filtering based on source and destination addresses, IPv6 option headers, and optional, upper-layer protocol type information for finer granularity of control. IPv6 access lists are defined by using the **ipv6 access-list** command in XR Config mode mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the router in IPv6 access list configuration mode—the router prompt changes to router (config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 access list.

See the “Examples” section for an example of a translated IPv6 access control list (ACL) configuration.

Note No more than one IPv6 access list can be applied to an interface per direction.

Note Every IPv6 access list has an implicit **deny ipv6 any any** statement as its last match condition. An IPv6 access list must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

Use the **ipv6 access-group** interface configuration command with the *access-list-name* argument to apply an IPv6 access list to an IPv6 interface.

Note An IPv6 access list applied to an interface with the **ipv6 access-group** command filters traffic that is forwarded, not originated, by the router.

Note Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.**permit icmp any any nd-na permit icmp any any nd-ns deny ipv6 any any deny ipv6 any any**.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to configure the IPv6 access list named list2 and applies the ACL to traffic on interface HundredGigE 0/2/0/2. Specifically, the first ACL entry keeps all packets from the network fec0:0:0:2::/64 (packets that have the site-local prefix fec0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of interface HundredGigE 0/2/0/2. The second entry in the ACL permits all other traffic to exit out of interface HundredGigE 0/2/0/2. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Router(config)# ipv6 access-list list2
Router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
Router(config-ipv6-acl)# 20 permit any any

Router# show ipv6 access-lists list2

ipv6 access-list list2
  10 deny ipv6 fec0:0:0:2::/64 any
  20 permit ipv6 any any

Router(config)# interface HundredGigE 0/2/0/2
```

Note IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from XR Config mode mode to IPv6 access list configuration mode.

Note An IPv6 router does not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

ipv6 access-list log-update rate

To specify the rate at which IPv6 access lists are logged, use the **ipv6 access-list log-update rate** command in XR Config mode. To return the update rate to the default setting, use the **no** form of this command.

ipv6 access-list log-update rate *rate-number*
no ipv6 access-list log-update rate *rate-number*

Syntax Description

rate-number	Rate at which IPv6 access hit logs are generated per second on the router. Range is 1 to 1000.

Command Default

Default is 1.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The *rate-number* argument applies to all the IPv6 access-lists configured on the interfaces. That is, at any given time there can be between 1 and 1000 log entries for the system.

Task ID

Task ID	Operations
ipv6	read, write
acl	read, write

Examples

This example shows how to configure a IPv6 access hit logging rate for the system:

```
Router(config)# ipv6 access-list log-update rate 10
```

ipv6 access-list log-update threshold

To specify the number of updates that are logged for IPv6 access lists (ACLs), use the **ipv6 access-list log-update threshold** command in XR Config mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv6 access-list log-update threshold *update-number*
no ipv6 access-list log-update threshold *update-number*

Syntax Description

update-number	Number of updates that are logged for every IPv6 access list configured on the router. Range is 0 to 2147483647.

Command Default

For IPv6 access lists, 350000 updates are logged.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ipv6 access-list log-update threshold** command is similar to the **ipv4 access-list log-update threshold** command, except that it is IPv6-specific.

IPv6 access list updates are logged at 5-minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

This example shows how to configure a log threshold of ten updates for every IPv6 access list configured on the router:

```
Router(config)# ipv6 access-list log-update threshold 10
```

is-fragment

To configure an ACL to match on the **is-fragment** flag.

fragment-type is-fragment {**capture** | **counter** | **log** | **log-input** | **set** | **udf** | **nexthop1** }

Syntax Description

capture	ACL matches on the **is-fragment** flag, and captures the matched packet.
counter	ACL matches on the **is-fragment** flag, and displays the counter for the matches.
log	ACL matches on the **is-fragment** flag and logs the matches.
log-input	ACL matches on the **is-fragment** flag and logs the matches, incuding on the input interface.
set	ACL matches on the **is-fragment** flag and sets a particular action on the matches.
udf	ACL matches on the **is-fragment** flag, and sets the user-defined fields for the matches.
nexthop1	ACL matches on the **is-fragment** flag, and then matches on the **nexthop1** flag.

Command Default

None

Command Modes

ACL configuration mode.

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

This command is supported only for IPv4 ACLs.

Example

Use the following sample configuration to match on the **is-fragment** flag.

```
/* Enter the global configuraton mode and configure an IPv4 access list */
Router# config
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit tcp any any

/* Configure an ACE to match on the is-fragment flag (indicates a fragmented packet)
 and forward the packet to a next hop of 10.10.10.1  */
Router(config-ipv4-acl)# 30 permit udp any any fragment-type is-fragment nexthop1 ipv4
192.0.2.1
Router(config-ipv4-acl)# commit
```

last-fragment

To configure an access list to match on the **last-fragment** flag.

fragment-type last-fragment {**capture** | **counter** | **log** | **log-input** | **set** | **udf** | **nexthop1** }

Syntax Description

capture	ACL matches on the **last-fragment** flag, and captures the matched packet.
counter	ACL matches on the **last-fragment** flag, and displays the counter for the matches.
log	ACL matches on the **last-fragment** flag and logs the matches.
log-input	ACL matches on the **last-fragment** flag and logs the matches, incuding on the input interface.
set	ACL matches on the **dont-fragment** flag and sets a particular action on the matches.
udf	ACL matches on the **last-fragment** flag, and sets the user-defined fields for the matches.
nexthop1	ACL matches on the **last-fragment** flag, and then matches on the **nexthop1** flag.

Command Default

None

Command Modes

ACL configuration mode.

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

This command is supported only for IPv4 ACLs.

Example

Use the following sample configuration to match on the **last-fragment** flag.

```
/* Enter the global configuraton mode and configure an IPv4 access list */
Router# config
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit tcp any any

/* Configure an ACE to match on the last-fragment flag (indicates the last fragment of a
fragmented packet)
 and forward the packet to a next hop of 30.30.30.1  */
Router(config-ipv4-acl)# 50 permit icmp any any fragment-type last-fragment nexthop1 ipv4
192.0.2.1
Router(config-ipv4-acl)# commit
```

object-group network

To configure a network object group, and to enter the network object group configuration mode, use the **object-group network** command in the global configuration mode. To de-configure the network object group, use the **no** form of this command.

object-group network { **ipv4 | ipv6** } *object-group-name*
no object-group network { **ipv4 | ipv6** } *object-group-name*

Syntax Description

ipv4	Configures the operation state of an IPV4 network object group.
ipv6	Configures the operation state of an IPV6 network object group.
object-group-name	Name of the object-group.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

Inherited object-groups up to four levels are supported in this release.

If an ACL is applied on an interface with non-zero compression level (implying it contains no ABF ACEs), a user cannot add an ACE with object-group.

Task ID

Task ID	Operation
system	read, write

Example

This example shows how to configure a network object-group, and to enter the network object-group configuration mode:

```
Router# configure
Router(config)# object-group network ipv4 ipv4_type5_obj1
Router(config-object-group-ipv4)#
```

object-group port

To configure a port object group, and to enter the port object group configuration mode, use the **object-group port** command in the global configuration mode. To de-configure the port object group, use the **no** form of this command.

object-group port *object-group-name*
no object-group port *object-group-name*

Syntax Description

object-group-name	Name of the object-group.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

Inherited object-groups upto four levels are supported.

Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

Task ID

Task ID	Operation
system	read, write

Example

This example show how to configure a port object-group, and to enter the port object-group configuration mode:

```
Router# configure
Router(config)# object-group port ipv4_type5_obj1
Router(config-object-group-port)#
```

packet-length

Enables filtering of packets at an ingress/egress interface by specifying the packet length as a match condition in a IPv4/IPv6 ACL.

By using the **packet-length** condition in an ACL, IPv4 and IPv6 packets are either processed (permit statement) or dropped (deny statement).

To remove this configuration, use the **no** prefix for the command.

packet-length { **eq** *value* | **gt** *value* | **lt** *value* | **neq** *value* | **range** *lower-limit upper-limit* }

Syntax Description

packet-length eq *value*	Filters packets that have a packet length equal to the specified limit.
packet-length gt *value*	Filters packets that have a packet length greater than the specified limit.
packet-length lt *value*	Filters packets that have a packet length less than the specified limit.
packet-length neq *value*	Filters packets that have a packet length that does not match the specified limit.
packet-length range *lower-limit upper-limit*	Filters packets that have a packet length within the specified range. The IPv4/IPv6 packet length ranges from 0 to 65535.

Command Default

None

Command Modes

Access List Configuration mode

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how you can configure an IPv4 access list with the **packet-length** condition.

```
Router# config
Router(config)# ipv4 access-list pktlen-v4
Router(config-ipv4-acl)# 10 permit tcp any any packet-length eq 1482
Router(config-ipv4-acl)# 20 permit udp any any packet-length range 1400 1500
Router(config-ipv4-acl)# 30 deny ipv4 any any
```

The following example shows how you can configure an IPv6 access list with the **packet-length** condition.

```
Router# config
Router(config)# ipv6 access-list pktlen-v6
Router(config-ipv6-acl)# 10 permit tcp any any packet-length eq 1500
Router(config-ipv6-acl)# 20 permit udp any any packet-length range 1500 1600
Router(config-ipv6-acl)# 30 deny ipv6 any any
```

permit (IPv4)

To set conditions for an IPv4 access list, use the **permit** command in access list configuration mode. There are two versions of the **permit** command: **permit** (source), **permit** (destination), and **permit** (protocol). To remove a condition from an access list, use the **no** form of this command.

[*sequence-number*] **permit** *source* [*source-wildcard*] [**log | log-input**]
[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**nexthop** [*ipv4-address1*] [*ipv4-address2*] [*ipv4-address3*]] [**dscp** *dscp* [**bitmask** *value*]] [**fragments**] [**log | log-input**] [**nexthop** [**track** *track-name*] [*ipv4-address1*] [*ipv4-address2*] [*ipv4-address3*] [**ttl** *ttl value* [*value1* **. . .** *value2*]]
no *sequence-number*

Internet Control Message Protocol (ICMP)
[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**]

Transmission Control Protocol (TCP)
[sequence-number] **permit tcp** { *source-ipv4-prefix/ prefix-length | any | host source-ipv4-address ipv4-wildcard-mask/prefix-length* } [*operator* { *port | protocol-port* }] { *destination-ipv4-prefix/ prefix-length | any | host destination-ipv4-address ipv4-wildcard-mask/prefix-length* } [*operator* { *port | protocol | port* }] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] { **match-any | match-all | + | -** } [*flag-name*] [**log**]

Internet Group Management Protocol (IGMP)
[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] [**fragments**]

User Datagram Protocol (UDP)
[*sequence-number*] **permit udp** *source source-wildcard* [*operator* {*portprotocol-port*}] *destination destination-wildcard* [*operator* {*portprotocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**]

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an IP protocol. It can be one of the keywords **ahp** , **esp** , **gre** , **icmp** , **igmp** , **igrp** , **ip** , **ipinip** , **nos** , **ospf** , **pim** , **pcp** , **tcp** , or **udp** , or an integer from 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. ICMP, and TCP allow further qualifiers, which are described later in this table. **Note** Filtering on AHP protocol is not supported.

destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
nexthop1, nexthop2, nexthop3	Specifies the next hop for this entry. **Note** You must specify the VRF for all nexthops unless the nexthop is in the default VRF.

precedence *precedence*	(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names: • **Routine** —Match packets with routine precedence (0) • **priority** —Match packets with priority precedence (1) • **immediate** —Match packets with immediate precedence (2) • **flash** —Match packets with flash precedence (3) • **flash-override** —Match packets with flash override precedence (4) • **critical** —Match packets with critical precedence (5) • **internet** —Match packets with internetwork control precedence (6) • **network** —Match packets with network control precedence (7)

dscp *dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • 0–63—Differentiated services codepoint value • af11—Match packets with AF11 dscp (001010) • af12—Match packets with AF12 dscp (001100) • af13—Match packets with AF13 dscp (001110) • af21—Match packets with AF21 dscp (010010) • af22—Match packets with AF22 dscp (010100) • af23—Match packets with AF23 dscp (010110) • af31—Match packets with AF31 dscp (011010) • af32—Match packets with AF32 dscp (011100) • af33—Match packets with AF33 dscp (011110) • af41—Match packets with AF41 dscp (100010) • af42—Match packets with AF42 dscp (100100) • af43–Match packets with AF43 dscp (100110) • cs1—Match packets with CS1 (precedence 1) dscp (001000) • cs2—Match packets with CS2 (precedence 2) dscp (010000) • cs3—Match packets with CS3 (precedence 3) dscp (011000) • cs4—Match packets with CS4 (precedence 4) dscp (100000) • cs5—Match packets with CS5 (precedence 5) dscp (101000) • cs6—Match packets with CS6 (precedence 6) dscp (110000) • cs7—Match packets with CS7 (precedence 7) dscp (111000) • default—Default DSCP (000000) • ef—Match packets with EF dscp (101110)

dscp range *dscp dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • 0–63—Differentiated services codepoint value • af11—Match packets with AF11 dscp (001010) • af12—Match packets with AF12 dscp (001100) • af13—Match packets with AF13 dscp (001110) • af21—Match packets with AF21 dscp (010010) • af22—Match packets with AF22 dscp (010100) • af23—Match packets with AF23 dscp (010110) • af31—Match packets with AF31 dscp (011010) • af32—Match packets with AF32 dscp (011100) • af33—Match packets with AF33 dscp (011110) • af41—Match packets with AF41 dscp (100010) • af42—Match packets with AF42 dscp (100100) • af43–Match packets with AF43 dscp (100110) • cs1—Match packets with CS1 (precedence 1) dscp (001000) • cs2—Match packets with CS2 (precedence 2) dscp (010000) • cs3—Match packets with CS3 (precedence 3) dscp (011000) • cs4—Match packets with CS4 (precedence 4) dscp (100000) • cs5—Match packets with CS5 (precedence 5) dscp (101000) • cs6—Match packets with CS6 (precedence 6) dscp (110000) • cs7—Match packets with CS7 (precedence 7) dscp (111000) • default—Default DSCP (000000) • ef—Match packets with EF dscp (101110)

fragments	(Optional) Causes the software to examine noninitial fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) **Note** ACL logging is supported only in ingress direction for both IPv4 and IPv6. The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches a flow, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
ttl value [*value1 ... value2*]	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.

icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.
igmp-type	(Optional) IGMP message type (0 to 15) or message name for filtering IGMP packets, as follows: • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report
operator	(Optional) Operator is used to compare source or destination ports. Possible operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* values, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* values, it must match the destination port. If the operator is positioned after the **ttl** keyword, it matches the TTL value. The **range** operator requires two port numbers. All other operators require one port number.
port	Decimal number a TCP or UDP port. Range is 0 to 65535. TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.

protocol-port	Name of a TCP or UDP port. TCP and UDP port names are listed in the "Usage Guidelines" section. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with + or - . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack** , **fin** , **psh** , **rst** , **syn** , **urg** .

Command Default

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.8.1	**log-input** keyword was introduced.
Release 7.5.4	**bitmask** keyword was introduced.

Usage Guidelines

Use the **permit** command following the **ipv4 access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without retyping the entire list. To add a new **s**tatement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

Note If any ACE in an ACL contains ABF clause, this ACL cannot be applied at any non-zero compression level.

The following is a list of precedence names:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The following is a list of ICMP message type names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big

- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs

- talk
- telnet
- time
- uucp
- whois
- www

The following UDP port names can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

Use the following flags in conjunction with the **match-any** and **match-all** keywords and the + and - signs to select the flags to display:

- ack
- fin
- psh
- rst
- syn

For example, **match-all** +*ack* +*syn* displays TCP packets with both the ack *and* syn flags set, or **match-any** +*ack* – - *syn* displays the TCP packets with the ack set *or* the syn not set.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to set a permit condition for an access list named Internetfilter:

```
Router(config)# ipv4 access-list Internetfilter
Router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
Router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
Router(config-ipv4-acl)# 25 permit tcp host 172.16.0.0 eq bgp host 192.168.202.203 range
1300 1400
Router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

This example shows how you can configure DSCP bitmask on ingress ERSPAN.

```
Router# config
Router(config)# ipv4 access-list acl1
Router(config-ipv4-acl)# 10 permit ipv4 host 192.0.2.1 any dscp af22 bitmask 0x3f
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit
Router(config)# interface HundredGigE0/0/0/6
Router(config-if)# ipv4 address 192.0.2.51 255.255.255.0
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv4 acl1
Router(config-if)# commit
```

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

[sequence-number] **permit** *source* { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } [*operator* { *port* | *protocol-port* }] [**dscp** *value* [**bitmask** *value*]] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log | log-input**]

[sequence-number] **permit** *protocol* { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length* } { *source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address* } [*operator* { *port* | *protocol-port* }] [**dscp** *value* [**bitmask** *value*]] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log | log-input**]

[`ttl` *ttl value* [*value1* . . . *value2*]]

no *sequence-number*

Internet Control Message Protocol (ICMP)

[sequence-number] **permit icmp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length*} {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address* } {*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/prefix-length*} [*icmp-type*] [*icmp-code*] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**log**]

Transmission Control Protocol (TCP)

[sequence-number] **permit tcp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/prefix-length*} [*operator* {*port* | *protocol* | *port*}] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] {**match-any | match-all | + | -**} [*flag-name*] [**log**]

User Datagram Protocol (UDP)

[sequence-number] **permit tcp** {*source-ipv6-prefix/ prefix-length* | *any* | *host source-ipv6-address ipv6-wildcard-mask/prefix-length*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/ prefix-length* | *any* | *host destination-ipv6-address ipv6-wildcard-mask/prefix-length*} [*operator* {*port* | *protocol* | *port*}] [**dscp** *value*] [**routing**] [**hop-by-hop**] [**authen**] [**destopts**] [**fragments**] [**established**] [*flag-name*] [**log**]

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. Range is from 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **gre** , **icmp**, **igmp**, **igrp**, **isinip**, **ipv6**, **nos**, **ospf**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer that ranges from 0 to 255, representing an IPv6 protocol number.
source-ipv6-prefix / *prefix-length*	Source IPv6 network or class of networks about which permit conditions are to be set. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	Source IPv6 host address about which to set permit conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-wildcard-mask	IPv6 wildcard mask. The IPv6 wildcard mask can take any IPv6 address value which is used instead of prefix length.

operator {*port* | *protocol-port*}	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix* / *prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix* / *prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The *port* argument is the decimal number of a TCP or UDP port. A port number is a number whose range is from 0 to 65535. The *protocol-port* argument is the name of a TCP or UDP port. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix / *prefix-length*	Destination IPv6 network or class of networks about which permit conditions are to be set. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	Specifies the destination IPv6 host address about which permit conditions are to be set. This *destination-ipv6-address* argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

dscp *value*	(Optional) Matches a differentiated services code point (DSCP) value against the traffic class value in the Traffic Class field of each IPv6 packet header. Range is from 0 to 63.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
hop-by-hop	(Optional) Supports Jumbo-grams. With the Router Alert option, it is an integral part in the operation of Multicast Listener Discovery (MLD). Router Alert [3] is an integral part in the operations of IPv6 Multicast through MLD and RSVP for IPv6.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The **fragments** keyword is an option available only if the *operator* [*port-number*] arguments are not specified.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) **Note** ACL logging is supported only in ingress direction for both IPv4 and IPv6. The message includes the access list name and sequence number, and whether the packet is permitted; the protocol, and whether it is TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first matching packet, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the log-message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value. For IPv6 packets, **ttl** is also referred to as hop limit.
ttl value [*value1 ... value2*]	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
operator	(Optional) Operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).

icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with + or - . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Required) For the TCP protocol **match-any**, **match-all**. Flag names are: **ack**, **fin**, **psh**, **rst**, **syn**, **urg**.

Command Default

ICMP message generation is enabled by default.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.2.1	Ingress IPv6 TCP flags are supported.
Release 7.3.15	Egress IPv6 TCP flags are supported.
Release 7.8.1	**log-input** keyword was introduced.
Release 7.8.1	**ttl** keyword was introduced.
Release 7.5.4	**bitmask** keyword was introduced.

Release	Modification
Release 7.10.1	IPv6 AHP and ESP headers are supported.

Usage Guidelines

The **permit** (IPv6) command is similar to the **permit** (IPv4) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list.

Specifying **ipv6** for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny, or remark** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, and not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option available only if the *operator* [*port* | *protocol-port*] arguments are not specified.

Task ID

Task ID	Operations
acl	read, write

Examples

This example shows how to configure the IPv6 access list named v6-abf-acl and apply the access list to inbound traffic on HundredGigE interface 0/0/2/0.

```
Router(config)# ipv6 access-list v6-abf-acl
Router(config-ipv6-acl)# 10 permit ipv6 any any
Router(config-ipv6-acl)# 20 permit ipv4 any any
Router(config)# interface HundredGigE 0/0/2/0
Router(config-if)# ipv6 access-group v6-abf-acl ingress
```

The following example shows how to configure the IPv6 access list named toCISCO and apply the access list to the traffic entering theHundredGigE interface 0/2/0/2. Specifically, the permit entry in the list allows all packets that have a hop-by-hop optional field from entering the HundredGigE interface 0/2/0/2.

```
Router(config)# ipv6 access-list toCISCO
Router(config-ipv6-acl)# permit ipv6 any any hop-by-hop
Router(config)#  interface HundredGigE 0/2/0/2
Router(config-if)# ipv6 access-group tOCISCO ingress
```

The following example shows how you can configure DSCP bitmask on ingress ERSPAN.

```
Router# config
Router(config)# ipv6 access-list acl1
Router(config-ipv6-acl)# 10 permit ipv6 host 2001:DB8::2/32 any dscp 33 bitmask 0x3f
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
Router(config)# interface HundredGigE 0/0/10/3
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# monitor-session TEST ethernet direction rx-only port-level acl ipv6 acl1
Router(config-if)# commit
```

The following example shows how you can configure AHP and ESP headers on an ACLs.

```
Router(config)# #ipv6 access-list ipv6_umpp_access_list
Router(config-ipv6-acl)# 12 permit ahp any any
Router(config-ipv6-acl)# ipv6 access-list ipv6_umpp_access_list
Router(config-ipv6-acl)# 14 permit esp any any
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# exit
```

show access-lists ipv4

To display the contents of current IPv4 access lists, use the **show access-lists ipv4** command in XR EXEC mode.

show access-lists ipv4 [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id* | [**usage pfilter** { **location** *node-id* }]}]

Syntax Description

access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain spaces or quotation marks, but can include numbers.
hardware	(Optional) Identifies the access list as an access list for an interface.
ingress	(Optional) Specifies an inbound interface.
interface	(Optional) Displays interface statistics.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
sequence *number*	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483644.
location *node-id*	(Optional) Location of a particular IPv4 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays a summary of all current IPv4 access lists.

sequence-number	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483644.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.

Command Default

The default displays all IPv4 access lists.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show access-lists ipv4** command to display the contents of all IPv4 access lists. To display the contents of a specific IPv4 access list, use the *name* argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **hardware , ingress** and **location** keywords to display the access list hardware contents and counters for all interfaces that use the specified access list in a given direction. To display the contents of a specific access list entry, use the **sequence** *number* keyword and argument. The access group for an interface must be configured using the **ipv4 access-group** command for access list hardware counters to be enabled.

Use the **show access-lists ipv4 summary** command to display a summary of all current IPv4 access lists. To display a summary of a specific IPv4 access list, use the *name* argument.

Use the **show access-list ipv4 usage** command to display a summary of all interfaces and access lists programmed on the specified line card.

Task ID

Task ID	Operations
acl	read

Examples

In the following example, the contents of all IPv4 access lists are displayed:

```
Router# show access-lists ipv4

ipv4 access-list test_ipv4
 10 permit ipv4 any any
 20 deny tcp any eq 2000 any eq 2000
 30 permit tcp any eq 3000 any eq 3000
```

This table describes the significant fields shown in the display.

Table 2: show access-lists ipv4 hardware Field Descriptions

Field	Description
hw matches	Number of hardware matches.
ACL name	Name of the ACL programmed in hardware.
Sequence Number	Each ACE sequence number is programmed into hardware with all the fields that are corresponding to the values set in ACE.
Grant	Depending on the ACE rule, the grant is set to deny, permit, or both.
Logging	Logging is set to on if ACE uses a log option to enable logs.
Per ace icmp	If Per ace icmp is set to on in the hardware, ICMP is unreachable, is rate-limited, and is generated. The default is set to on.
Hits	Hardware counter for that ACE.

In the following example, a summary of all IPv4 access lists are displayed:

```
Router# show access-lists ipv4 summary

ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

This table describes the significant fields shown in the display.

Table 3: show access-lists ipv4 summary Field Descriptions

Field	Description
Total ACLs configured	Number of configured IPv4 ACLs.
Total ACEs configured	Number of configured IPV4 ACEs.

This example displays the packet filtering usage for the specified line card:

```
Router# show access-lists ipv4 usage pfilter location 0/RP0/CPU0

 Interface : HundredGigE0/0/0/10/0
Input ACL : Common-ACL : N/A ACL : test_ipv4
Output ACL : N/A
```

Note To display the packet filtering usage for bundle interfaces, use the **show access-lists ipv4 usage pfilter location all** command.

show access-lists ipv6

To display the contents of current IPv6 access lists, use the **show access-lists ipv6** command in XR Config mode.

show access-lists ipv6 [*access-list-name* **hardware** {**ingress** | **egress**} [**interface** *type interface-path-id*] {**sequence** *number* | **location** *node-id* | [**usage pfilter** { **location** *node-id* }]}]

Syntax Description

access-list-name	(Optional) Name of a particular IPv6 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
hardware	(Optional) Identifies the access list as an access list for an interface.
ingress	(Optional) Specifies an inbound interface.
interface	(Optional) Displays interface statistics.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
sequence *number*	(Optional) Sequence number of a particular IPv6 access list. Range is 1 to 2147483644.
location *node-id*	(Optional) Location of a particular IPv6 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays a summary of all current IPv6 access lists.
sequence-number	(Optional) Sequence number of a particular IPv6 access list. Range is 1 to 2147483644.
usage	(Optional) Displays the usage of the access list on a given line card.

pfilter	(Optional) Displays the packet filtering usage for the specified line card.
all	(Optional) Displays the location of all the line cards.

Command Default

Displays all IPv6 access lists.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show access-lists ipv6** command is similar to the **show access-lists ipv4** command, except that it is IPv6 specific.

Use the **show access-lists ipv6** command to display the contents of all IPv6 access lists. To display the contents of a specific IPv6 access list, use the *name* argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **hardware , ingress** and **location** keywords to display the access list hardware contents and counters for all interfaces that use the specified access list in a given direction. To display the contents of a specific access list entry, use the **sequence** *number* keyword and argument. The access group for an interface must be configured using the **ipv6 access-group** command for access list hardware counters to be enabled.

Use the **show access-lists ipv6 summary** command to display a summary of all current IPv6 access lists. To display a summary of a specific IPv6 access list, use the *name* argument.

Use the **show access-list ipv6 usage** command to display a summary of all interfaces and access lists programmed on the specified line card.

Task ID

Task ID	Operations
acl	read

Examples

In the following example, the IPv6 ACL is configured with the source IPv6 wildcard mask FF:0:FFFF:AA:20 and the destination wildcard mask 0:FFFF:2233::FFFF, the show command displays these wildcard mask:

```
Router# config
Router(config)# ipv6  access-list acl1
Router(config-ipv6-acl)# permit 1:2::3 FF:0:FFFF:AA:20:: 4:5::6 0:FFFF:2233::FFFF
Router(config-ipv6-acl)# commit
Router# show run ipv6 access-list
ipv6 access-list ACL1
 10 permit ipv6 1:2::3 ff:0:ffff:aa:20:: 4:5::6 0:ffff:2233::ffff
```

In the following example, the contents of all IPv6 access lists are displayed:

```
Router# show access-lists ipv6

ipv6 access-list test_ipv6
```

```
 10 permit ipv6 any any
 20 permit tcp any eq 3000 any eq 3000
```

In the following example, the contents of an access list named Internetfilter is displayed:

```
Router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  3 remark Block BGP traffic from a given host
  4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
  20 permit ipv6 3333:1:2:3::/64 any
  25 permit ipv6 4444:1:2:3::/64 any
  30 permit ipv6 5555:1:2:3::/64 any
```

This table describes the significant fields shown in the display.

Table 4: show access-lists ipv6 hardware Command Field Descriptions

Field	Description
hw matches	Number of hardware matches.

In the following example, a summary of all IPv6 access lists is displayed:

```
Router# show access-lists ipv6 summary

ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

This table describes the significant fields shown in the display.

Table 5: show access-lists ipv6 summary Command Field Descriptions

Field	Description
Total ACLs configured	Number of configured IPv6 ACLs.
Total ACEs configured	Number of configured IPV6 ACEs.

In the following example, the OOR details of the IPv6 access lists are displayed:

```
Router# show access-lists ipv6 maximum detail

Default max configurable acls :1000
Default max configurable aces :50000
Current configured acls       :1
Current configured aces       :2
Current max configurable acls :1000
Current max configurable aces :50000
Max configurable acls         :2000
Max configurable aces         :100000
```

This example displays the packet filtering usage for the specified line card:

```
Router# show access-lists ipv6 usage pfilter location 0/0/CPU0

Interface : HundredGigE0/0/0/10/0
    Input  ACL : Common-ACL : N/A  ACL : test_ipv6
    Output ACL : N/A
```

show tech-support access-lists

To automatically collect information about Ethernet Services, IPV4, IPV6, and Platform dependent ACL related information, use the **show tech-support access-lists** command in configuration mode.

show tech-support access-lists { **ethernet-services** | **ipv4** | **ipv6** | **platform** }

Syntax Description

ethernet-services	Collects information regarding the ethernet-services access lists in the router.
ipv4	Collects information regarding the ipv4 access lists in the router.
ipv6	Collects information regarding the ipv6 access lists in the router.
platform	Collects information regarding the platform specific access lists in the router.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

- To use commands, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.
- This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. By default, the output of this command is saved on the router's hard disk in a file with *.tgz* extension. You can share this file with Cisco Technical Support. To share, use the **copy** command to copy the *.tgz* file to a server or local machine. For example, **copy harddisk:/showtech/** *name.tgz* **tftp://** *server_path* .
- This command is not required during normal use of the router.

Task ID

Task ID	Operations
acl	read

Examples

The following example shows the output of the **show tech-support access-lists** command:

```
Router# show tech-support access-lists ipv4
Thu Oct 20 10:38:18.041 PDT
++ Show tech start time: 2022-Oct-20.103818.PDT ++
Thu Oct 20 10:38:18 PDT 2022 Waiting for gathering to complete
.....
Thu Oct 20 10:38:33 PDT 2022 Compressing show tech output
Show tech output available at 0/RP0/CPU0 :
/harddisk:/showtech/showtech-M8102TOR1-ipv4-acl-2022-Oct-20.103818.PDT.tgz
++ Show tech end time: 2022-Oct-20.103833.PDT ++
```

tcam format access-list (ipv4 and ipv6)

To configure the object group ACLs for IPv4 and IPv6 using the user-defined TCAM keys (UDK), use the **hw-module profile tcam format access-list ipv4** command and **hw-module profile tcam format access-list ipv6** in XR Config mode.

Syntax for IPv4:

hw-module profile tcam format access-list ipv4

Syntax Description

dst-addr	Specifies destination address. This is a 32-bit qualifier for IPv4 ACLs.
dst-object-group	Specifies the destination object group.
dst-port	Destination port for TCP/UDP. This is a 16-bit qualifier.
frag-bit	Fragmentation bit for IPv4 ACLs. This is a 1-bit qualifier.
fragment-offset	Specifies the fragment offset for IPv4 ACLs.
packet-len	Specifies packet length for IPv4 ACLs. This is a 10-bit qualifier.
precedence	Specifies DSCP precedence in IPv4 header. This is a 10-bit qualifier.
proto	Specifies protocol type in IPv4 header. This is an 8-bit qualifier.
src-addr	Specifies source address. This is a 32-bit qualifier for IPv4 ACLs.
src-object-group	Specifies the source object group.
src-port	Specifies source port for TCP/UDP. This is a 16-bit qualifier.
tcp-flags	Specifies TCP Flags. This is a 6-bit qualifier for IPv4 ACLs.

Syntax for IPv6:

hw-module profile tcam format access-list ipv6

Syntax Description

dst-addr	Specifies destination address. This is a 128-bit qualifier for IPv6 ACLs.
dst-object-group	Specifies the destination object group.
dst-port	Destination port for TCP/UDP. This is a 16-bit qualifier.
frag-bit	Fragmentation bit for IPv6 ACLs. This is a 1-bit qualifier.
next-hdr	(Mandatory) Specifies the next header field in IPv6 header. This is an 8-bit qualifier.
packet-len	Specifies packet length for IPv6 ACLs. This is a 10-bit qualifier.
src-addr	Specifies source address. This is a 128-bit qualifier for IPv6 ACLs.
src-object-group	Specifies the source object group.

src-port	(Mandatory) Specifies source port for TCP/UDP. This is a 16-bit qualifier.
tcp-flags	Specifies TCP Flags. This is an 8-bit qualifier for IPv6 ACLs.
traffic-class	Specifies traffic class in IPv6 header. This is an 8-bit qualifier for IPv6 ACLs.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 24.2.1	These commands were introduced.

Usage Guidelines

- Remove all ACL attachments to interfaces before the IPv4/IPv6 UDK configuration.
- Make sure that you reload the line card for this configuration to take effect.

Task ID

Task ID	Operations
acl	read, write
ipv4	read, write
ipv6	read, write

Examples

Example 1: In UDK, if only the **dst-object-group** is specified and the **src-object-group** is not specified, you compress only the destination address (compress level 4) as shown in this example.

```
Router(config)# hw-module profile tcam format access-list ipv4 src-addr src-port dst-port
proto tcp-flags frag-bit dst-object-group
Router(config)# hw-module profile tcam format access-list ipv6 src-addr src-port dst-port
next-hdr frag-bit tcp-flags dst-object-group
```

```
interface FH0/0/0/1
 RP/0/RP0/CPU0:ios(config-if)#ipv6 access-group v6-test ingress compress level 4
```

Example 2: In UDK, if only the **src-object-group** is specified and the **dst-object-group** is not specified, you compress only the source address (compress level 1) as shown in this example.

```
Router(config)# hw-module profile tcam format access-list ipv4 src-object-group src-port
dst-port proto tcp-flags frag-bit dst-addr
Router(config)# hw-module profile tcam format access-list ipv6 src-object-group src-port
dst-port next-hdr frag-bit tcp-flags dst-addr
```

```
interface FH0/0/0/1
 RP/0/RP0/CPU0:ios(config-if)#ipv4 access-group v4-test ingress compress level 1
```

Note By default, compression level 2 is supported for both the **src-object-group** and **dst-object-group** without the UDK configuration.

ARP Commands

This chapter describes the commands used to configure and monitor the Address Resolution Protocol (ARP) on Cisco 8000 Series Routers.

For detailed information about ARP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

arp

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in XR Config mode. To remove an entry from the ARP cache, enter the **no** form of this command.

arp [**vrf** *vrf-name*] *ip-address* *hardware-address* *encapsulation-type* [**alias**]
no **arp** [**vrf** *vrf-name*] *ip-address* *hardware-address* *encapsulation-type* [**alias**]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF instance that identifies a VPN.
ip-address	IPv4 (network layer) address for which a permanent entry is added to the ARP cache. Enter the IPv4 address in a four-part dotted-decimal format that corresponds to the local data-link address (a 32-bit address).
hardware-address	Hardware (data link layer) address that the IPv4 address is linked to. Enter the local data-link address (a 48-bit address), such as 0800.0900.1834.
encapsulation-type	Encapsulation type. The encapsulation types are: • arpa • srp • srpa • srpb For Ethernet interfaces, this is typically the arpa keyword.
alias	(Optional) Causes the software to respond to ARP requests as if it were the owner of both the specified IP address and hardware address, whether proxy ARP is enabled or not.

Command Default

No entries are permanently installed in the ARP cache.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries.

Static entries are permanent entries that map a network layer address (IPv4 address) to a data-link layer address (MAC address). If the **alias** keyword is specified when creating the entry, the interface to which the entry is attached will act as if it is the owner of the specified addresses, that is, it will respond to ARP request packets for this network layer address with the data link layer address in the entry.

The software does not respond to any ARP requests received for the specified IP address unless proxy ARP is enabled on the interface on which the request is received. When proxy ARP is enabled, the software responds to ARP requests with its own local interface hardware address.

To remove all nonstatic entries from the ARP cache, enter the `clear arp-cache` in XR EXEC mode.

Task ID

Task ID	Operations
cef	read, write

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
Router# configure
Router(config)# arp 192.168.7.19 0800.0900.1834 arpa
```

arp cache-limit

To configure a limit on ARP cache entries on the router, use the **arp cache-limit** command in interface configuration mode.

arp cache-limit *limit*

Syntax Description

limit	Specify the value for the cache entries. The supported range in the router is 0–127999. **Note** The arp cache resources vary depending on the hardware resources available in a router. Ensure the cache-limit configured such that the available resources in the router are able to accomodate the entries.

Command Default

By default, the ARP cache limit per interface in the router is 127999.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.9.1	This command was introduced.
Release 7.5.4	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

The following example shows how to set the ARP cache limit for an interface:

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/0
Router(config-if)#arp cache-limit 3900
Router(config-if)#commit
```

arp dagr

To configure Direct Attached Gateway Redundancy (DAGR), use the **arp dagr** command in interface configuration mode.

arp dagr

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
cef	write

Examples

The following example enables DAGR configuration:

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/0
Router(config-if)# arp dagr
Router(config-if-dagr)#
```

arp gratuitous ignore

To ignore receipt of gratuitous Address Resolution Protocol (ARP) packets, use the **arp gratuitous ignore** command in interface configuration mode. To receipt gratuitous ARP packets, use the no form of this command.

arp gratuitous ignore
no arp gratuitous ignore

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	write

Examples

This example shows how to configure **arp gratuitous ignore** command:

```
Router# configure
Router(config)# interface HundredGigE 0/1/0/0
Router(config-if)# arp gratuitous ignore
```

arp learning

To enable the dynamic learning of ARP entries for a local subnet or all subnets, use the **arp learning** command.

To disable this command, use the **no** prefix or the **disable** option for this command.

arp learning local
no arp learning local
arp learning disable
no arp learning disable

Syntax Description

local	Enables the dynamic learning of ARP entries for local subnets. When arp learning local is configured on an interface or sub-interface, it learns only the ARP entries from ARP packets on the same subnet.
disable	Disables the dynamic learning of all ARP entries.

Command Default

This command has no keywords or arguments.

Command Modes

Sub-interface configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	write

The following example shows how to configure **arp learning local** command that enables the learning of ARP entries for only the local subnet:

```
Router(config)#interface HundredGigE 0/0/0/1
Router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)# arp learning local
Router(config-if)# no shut
Router(config-if)# commit
```

The following example shows how to configure **arp learning disable** command that disables the learning of all ARP entries.

```
Router(config)# interface HundredGigE 0/0/0/1
Router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)# arp learning disable
Router(config-if)# commit
```

arp purge-delay

To delay purging Address Resolution Protocol (ARP) entries when an interface goes down, use the **arp purge-delay** command in interface configuration mode. To turn off the purge delay feature, use the **no** form of this command.

arp purge-delay *value*
no arp purge-delay *value*

Syntax Description

value	Sets the purge delay time in seconds. Range is 1 to 65535.

Command Default

Default value is off.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **arp purge-delay** command to delay purging ARP entries when an interface goes down. If the interface comes up within the delay time, then the ARP entries are restored to prevent packet loss with Equal Cost Multipath (ECMP) configured.

Task ID

Task ID	Operations
cef	read, write

Examples

The following is an example of setting the purge delay to 50 seconds:

```
Router# configure
Router(config)# interface HundredGigE 0/0/0/0
Router(config-if)# arp purge-delay 50
```

arp timeout

To specify the duration of dynamic entries learned on an interface remain in the Address Resolution Protocol (ARP) cache, enter the **arp timeout** command in interface configuration mode. To remove the **arp timeout** command from the configuration file and restore the system to its default condition with respect to this command, enter the **no** form of this command.

arp timeout *seconds*
no arp timeout *seconds*

Syntax Description

seconds	Indicates the time, in seconds, for which an entry remains in the ARP cache. Range is 30 to 4294967295.

Command Default

Entries remain in the ARP cache for 14,400 seconds (4 hours).

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was supported.

Usage Guidelines

This command is ignored when issued on interfaces that do not use ARP. Also, ARP entries that correspond to the local interface or that are statically configured by the user never time out.

The **arp timeout** command applies only to the interface that is entered. When the timeout is changed for an interface the change applies only to that interface.

The **show interfaces** command displays the ARP timeout value in hours:minutes:seconds, as follows:

```
ARP type: ARPA, ARP Timeout 04:00:00
```

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows how to set the ARP timeout to 3600 seconds to allow entries to time out more quickly than the default:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#
RP/0/RP0/CPU0:router(config-if)# arp timeout 3600
```

clear arp-cache

To delete all dynamic entries from the Address Resolution Protocol (ARP) cache, clear the fast-switching cache, and clear the IP route cache, use the **clear arp-cache** command in XR EXEC mode.

clear arp-cache {**traffic** *type interface-path-id* | **location** *node-id*}

Syntax Description

traffic	Deletes traffic statistics on the specified interface.
t ype	Interface type. For more information, use the question mark (?) online help function.
interface- path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	Clears the ARP entries for a specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When issued without keywords or arguments, the **clear arp-cache** command clears all entries in the ARP cache.

Task ID

Task ID	Operations
cef	execute

Examples

The following example shows how to remove traffic statistic entries from the ARP cache that match the specified interface:

```
Router# clear arp-cache traffic HundredGige 0/1/0/0 location 0/1/CPU0
```

The following example shows how to remove entries from the ARP cache that match the specified location:

```
Router# clear arp-cache location 0/1/CPU0
```

local-proxy-arp

To enable local proxy Address Resolution Protocol (ARP) on an interface, enter the **local-proxy-arp** command in interface configuration mode. To disable local proxy ARP on the interface, enter the **no** form of this command.

local-proxy-arp
no local-proxy-arp

Syntax Description

This command has no keywords or arguments.

Command Default

Local proxy ARP is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When local proxy ARP is enabled, the networking device responds to ARP requests that meet all the following conditions:

- The target IP address in the ARP request, the IP address of the ARP source, and the IP address of the interface on which the ARP request is received are on the same Layer 3 network.
- The next hop for the target IP address is through the same interface as the request is received.

Typically, local proxy ARP is used to resolve MAC addresses to IP addresses in the same Layer 3 network such as, private VLANs that are Layer 2-separated. Local proxy ARP supports all types of interfaces supported by ARP and unnumbered interfaces.

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command.

Task ID

Task ID	Operations
cef	read, write

peer (DAGR)

To create a Direct Attached Gateway Redundancy (DAGR) group for a virtual IP address, use the **peer** command in DAGR interface configuration mode.

peer **ipv4** *IP-address*

Syntax Description

IP-address	Virtual IPv4 address for the DAGR group.

Command Default

None

Command Modes

DAGR interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer:

```
Router(config-if-dagr)# peer ipv4 192.168.7.19
Router(config-if-dagr-peer)#
```

priority-timeout

To configure the timer to time out a high-priority Direct Attached Gateway Redundancy (DAGR) route and reverting to normal priority, use the **priority-timeout** command in DAGR peer interface configuration mode.

priority-timeout *time*

Syntax Description

time	Time in seconds after which a high-priority route reverts to a normal priority route. The range of values is 1 to 10000.

Command Default

Default for *time* is 20 seconds.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When this function is applied, the DAGR group configuration is updated in the database.

The new timer values take effect the next time the timer is set. No immediate timer restarts are triggered on the basis of this event.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a priority timeout of 25 seconds:

```
Router(config-if-dagr-peer)# priority-timeout 25
Router(config-if-dagr-peer)#
```

proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, enter the **proxy-arp** command in interface configuration mode. To disable proxy ARP on the interface, enter the **no** form of this command.

proxy-arp
no proxy-arp

Syntax Description

This command has no keywords or arguments.

Command Default

Proxy ARP is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When proxy ARP is disabled, the networking device responds to ARP requests received on an interface only if one of the following conditions is met:

- The target IP address in the ARP request is the same as the interface IP address on which the request is received.
- The target IP address in the ARP request has a statically configured ARP alias.

When proxy ARP is enabled, the networking device also responds to ARP requests that meet all of the following conditions:

- The target IP address is not on the same physical network (LAN) on which the request is received.
- The networking device has one or more routes to the target IP address.
- All of the routes to the target IP address go through interfaces other than the one on which the request is received.

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command.

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows how to enable proxy ARP on HundredGigE interface 0/0/0/0:

```
Router#(config)# interface  HundredGigE 0/0/0/0
Router#(config-if)# proxy-arp
```

route distance

To configure route distance for a given Direct Attached Gateway Redundancy (DAGR) group, use the **route distance** command in DAGR peer interface configuration mode.

route distance normal *normal-distance* **priority** *priority-distance*

Syntax Description

normal *normal-distance*	Sets normal route (administrative) distance. Range is 0 to 256.
priority *priority-distance*	Sets priority route (administrative) distance. Range is 0 to 256.

Command Default

Default for *normal-distance* default is 150 and the default for *priority-distance* is 5.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The default setting for a priority distance takes precedence over that of a typical Internet Gateway Protocol (IGP). The normal distance setting does not.

When this setting is applied, the DAGR group is updated in the database.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer with a normal route distance of 48 and priority route distance of 5:

```
Router(config-if-dagr-peer)# route distance normal 48 priority 5
Router(config-if-dagr-peer)#
```

route metric

To configure normal and priority route metrics for a given Direct Attached Gateway Redundancy (DAGR) group, use the **route metric** command in DAGR peer interface configuration mode.

route metric normal *normal-metric* **priority** *priority-metric*

Syntax Description

normal *normal-metric*	Sets a normal value for routes installed in the Routing Information Base (RIB). The range of values is 0 to 256.
priority *priority-metric*	Sets a priority value for routes installed in the RIB. The range of values is 0 to 256.

Command Default

The default for *normal-metric* is 100, and the default for *priority-metric* is 90.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The route metric values are of less significance than the **route distance** command values. Setting a route metric allows the configuration of values for routers installed in the RIB.

When this setting is applied, the DAGR group is updated in the database.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer with a normal metric of 48 and a priority metric of 5:

```
Router(config-if-dagr-peer)# route metric normal 48 priority 5
Router(config-if-dagr-peer)#
```

show arp

To display the Address Resolution Protocol (ARP), enter the **show arp** command in XR EXEC mode.

show arp `vrf` *vrf-name* [*ip-address hardware-address interface-path-id*] **location** *node-id*

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF instance that identifies a VPN.
ip-address	(Optional) The ARP entries you want to display.
hardware-address	(Optional) The ARP entries that match the 48-bit MAC address are displayed.
interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays the ARP entry for a specific location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The active RSP is the default location.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and Ethernet hardware addresses. A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

For **show arp** *interface-type interface-instance* form, the **location** *node-id* keyword and argument is mandatory for Bundle and VLAN-on-Bundle interfaces to indicate which location the cache entries for the bundle should be displayed. For physical interfaces, specifying the **location** *node-id* keyword and argument is optional since the interface can only exist on one node.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show arp** command with no location specified:

```
Router# show arp

0/7/CPU0
-------------------------------------------------------------------------------
Address         Age        Hardware Addr    State      Type   Interface
192.1.1.2         -         e4c7.2284.f863   Interface  ARPA   HundredGigE0/7/0/3
192.1.1.2         -         e4c7.2284.f863   Interface  ARPA   HundredGigE0/7/0/3.1
192.79.1.1        -         e4c7.2284.f887   Interface  ARPA   HundresGigE0/7/0/39

-------------------------------------------------------------------------------
0/RP0/CPU0
-------------------------------------------------------------------------------
Address         Age        Hardware Addr    State      Type   Interface
203.1.24.208     00:00:03  0016.9cf2.3800   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.0.1        00:53:00  0000.0c07.ac07   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.0.2        00:00:01  0026.0bdd.0000   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.0.3        00:00:05  0026.0bdc.ffc0   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.13.2       02:41:25  0015.17d6.684b   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.36.19      00:33:28  0014.a841.0ffc   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.44.1       00:54:57  6c20.5618.96aa   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.44.2       01:46:47  6c20.5618.982e   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.44.3       02:46:28  4c4e.35b6.57e8   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.44.100     02:45:10  4c4e.35b6.57e8   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.44.101     02:45:05  6c20.5618.96aa   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.49.41      00:03:16  6400.f142.134c   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.49.43      01:10:36  6400.f142.134c   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.49.121     02:54:42  0020.b007.6700   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.49.122     01:51:05  0020.b007.6700   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.49.123     00:31:59  0033.b515.68ff   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.49.254     00:24:09  0003.310a.a039   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.54.10         -      e050.07fa.ef05   Interface   ARPA MgmtEth0/RP0/CPU0/0
203.7.54.11         -      e050.07fa.ef05   Interface   ARPA MgmtEth0/RP0/CPU0/0
203.7.54.12      01:24:34  4c4e.35b6.4af8   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.1       00:06:21  10f3.11b6.c634   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.2       00:05:58  6400.f142.1500   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.8       01:59:01  0024.c4d8.c2cc   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.9       00:54:16  6400.f142.0bbe   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.10      01:25:07  6400.f142.115a   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.11      00:59:03  0022.56d8.36a0   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
203.7.57.13      00:22:16  000a.b8b7.fff8   Dynamic     ARPA MgmtEth0/RP0/CPU0/0
```

The following is sample output from the **show arp** command with the *interface-type interface-instance* argument:

```
Router# show arp HundredGigE 0/0/0/1

-------------------------------------------------------------------------------
0/RP0/CPU0
-------------------------------------------------------------------------------
Address         Age        Hardware Addr   State      Type  Interface
20.30.1.1       -          c472.95a6.2a86  Interface  ARPA  HundredGigE0/0/0/1
20.30.1.2       00:04:58   6c9c.ed2c.a060  Dynamic    ARPA  HundredGigE0/0/0/1
```

```
Router# show arp mgmtEth 0/RP1/CPU0/0

Address      Age        Hardware Addr    State     Type   Interface
192.4.9.2     00:35:55   0030.7131.abfc   Dynamic   ARPA   MgmtEth0/RP1/CPU0/0
192.4.9.1     00:35:55   0000.0c07.ac24   Dynamic   ARPA   MgmtEth0/RP1/CPU0/0
192.4.9.99    00:49:12   0007.ebea.44d0   Dynamic   ARPA   MgmtEth0/RP1/CPU0/0
192.4.9.199     -        0001.c9eb.dffe   Interface ARPA   MgmtEth0/RP1/CPU0/0
```

The following is sample output from the **show arp** command with the *hardware-address* designation:

```
Router# show arp 0005.5f1d.8100

Address Age Hardware Addr State Type Interface
192.16.7.2 - 0005.5f1d.8100 Interface ARPA HundredGigE0/0/0/2
```

The following is sample output from the **show arp** command with the **location** keyword and *node-id* argument:

```
Router# show arp location 0/2/CPU0

Address Age Hardware Addr State Type Interface
192.168.15.1 - 00dd.00ee.00ff Alias ARPA
192.168.13.1 - 00aa.00bb.00cc Static ARPA
203.16.7.1 00:35:49 0002.fc0e.9600 Dynamic ARPA HundredGigE0/1/0/2
203.16.7.2 - 0005.5f1d.8100 Interface ARPA HundredGigE0/1/0/2
```

This table describes the significant fields shown in the display.

Table 6: show arp Command Field Descriptions

Field	Description
Address	Displays the network address that corresponds to the hardware address.
Age	Displays the age in hours:minutes:seconds of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	Displays the LAN hardware address of a MAC address that corresponds to the network address.
State	Displays the current state of the cache entry. Values are: • Dynamic • Interface • Alias • Static • "-" (indicates global static and alias entries)
Type	Displays the encapsulation type the Cisco IOS XR software is using for the network address in this entry. Value is ARPA.
Interface	Displays the interface associated with this network address.

Field	Description
ARP statistics	Displays ARP packet and error statistics.
ARP cache	Displays general information about the IP address and MAC address association entries in the ARP cache.
IP Packet drop count for node */*/*	Displays the number of IP packets dropped because the buffer ran out of space before an ARP response was received. **Note** */*/* represents the node ID in the format *rack/slot/module*.

show arp idb

To display the ARP database statistics for an interface, use the **show arp idb** command in EXEC mode.

show arp idb *interface-name* **location** *node-id*

Syntax Description

interface-name	Name of the interface
node-id	Location of the interface. LC node for physical interfaces, RP or LC node for virtual interfaces

Command Default

There is no default location, location needs to be provided in the CLI.

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

The **show arp idb** command is useful to verify the IP addresses, Mac address, ARP configuration(s) applied on the interface and the entry statistics.

For **show arp idb** *interface-type interface-instance* form, the **location** *node-id* keyword and argument is mandatory for Bundle and VLAN-on-Bundle interfaces to indicate which location the cache entries for the bundle should be displayed.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show arp idb** command:

```
RP/0/0/CPU0:ios#show arp idb GigabitEthernet 0/0/0/0 location 0/0/CPU0
Mon Jan 30 10:32:15.387 IST
GigabitEthernet0/0/0/0 (0x00000060):
IDB Client: default
IPv4 address 1.1.1.1, Vrf ID 0x60000000
VRF Name default
Dynamic learning: Enable
Dynamic entry timeout: 14400 secs
Drop adjacency timeout: Disable
Purge delay: off
Cache limit: 128000
Incomplete glean count: 1
```

```
Complete glean count: 0
Complete protocol count: 0
Dropped glean count: 0
Dropped protocol count: 0
IPv4 caps added (state up)
MPLS caps not added
Interface not virtual, not client fwd ref,
Proxy arp not configured, not enabled
Local Proxy arp not configured
Packet IO layer is NetIO
Srg Role : DEFAULT
Idb Flag : 49292
IDB is Complete
IDB Flag Description:
[CAPS | COMPLETE | IPV4_CAPS_CREATED | SPIO_ATTACHED |
SPIO_SUPPORTED]
Idb Flag Ext : 0x0
Idb Oper Progress : NONE
Client Resync Time : Jan 30 10:07:10.736787
Total entries : 9
| Event Name | Time Stamp | S, M
| idb-create | Jan 30 10:07:10.784 | 1, 0
| idb-state-up | Jan 30 10:07:10.784 | 0, 0
| caps-state-update | Jan 30 10:07:10.784 | 0, 1
| address-update | Jan 30 10:07:10.784 | 0, 0
| idb-complete | Jan 30 10:07:10.784 | 0, 0
| idb-entry-create | Jan 30 10:07:10.784 | 0, 0
| idb-caps-add | Jan 30 10:07:10.784 | 0, 0
| idb-caps-add-cb | Jan 30 10:07:10.784 | 0, 0
| idb-last-garp-sent | Jan 30 10:07:11.808 | 0, 0
```

show arp dagr

To display the operational state of all Direct Attached Gateway Redundancy (DAGR) groups, use the **show arp dagr** command in XR EXEC mode

show arp dagr [*interface* [*IP-address*]]

Syntax Description

interface [*IP-address*]	(Optional) Restricts the output to a specific interface and virtual IP address.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows the current operational state of the DAGR groups:

```
Router# show arp dagr

--------------------------------------------------------------------------------
0/1/CPU0
--------------------------------------------------------------------------------
Interface                 Virtual IP      State     Query-pd Dist Metr
HundredGigE0/1/0/2    192.0.2.1    Active    None     150  100
HundredGigE0/1/0/2    192.24.0.45     Query     1        None None
HundredGigE0/1/0/3    192.66.0.45     Init      None     None None
```

show arp traffic

To display Address Resolution Protocol (ARP) traffic statistics, enter the **show arp traffic** command in XR EXEC mode.

show arp traffic [**vrf** *vrf-name*] [*interface-path-id*] [**location** *node-id*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF instance that identifies a VPN.
interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays the ARP entry for a specific location. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The active RSP is the default location.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and Ethernet hardware addresses. A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

For **show arp traffic,** *interface-instance*, the **location***node-id* keyword and argument is mandatory for Bundle and VLAN-on-Bundle interfaces to indicate which location the cache entries for the bundle should be displayed. For physical interfaces, specifying the **location** *node-id* keyword and argument is optional since the interface can only exist on one node.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show arp traffic** command:

```
Router# show arp traffic

show arp traffic
Thu Dec 10 09:51:38.761 UTC

-------------------------------------------------------------------------------
0/6/CPU0
-------------------------------------------------------------------------------

ARP statistics:
  Recv: 163 requests, 79 replies
  Sent: 14138 requests, 177 replies (0 proxy, 0 local proxy, 14 gratuitous)
  Resolve requests rcvd: 7204
  Resolve requests dropped: 295
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 22
  Dynamic: 11, Interface: 11, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0

  IP Packet drop count for node 0/6/CPU0: 6909

  Total ARP-IDB:19


-------------------------------------------------------------------------------
0/2/CPU0
-------------------------------------------------------------------------------

ARP statistics:
  Recv: 162532 requests, 243 replies
  Sent: 15879 requests, 162561 replies (0 proxy, 0 local proxy, 29 gratuitous)
  Resolve requests rcvd: 47593
  Resolve requests dropped: 0
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 125
  Dynamic: 112, Interface: 13, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0

  IP Packet drop count for node 0/2/CPU0: 44804

  Total ARP-IDB:13
```

The following is sample output from the **show arp traffic** command with the **location** keyword and *node-id* argument:

```
Router# show arp traffic location 0/4/CPU0

Thu Dec 10 09:51:56.209 UTC
```

```
ARP statistics:
  Recv: 364474 requests, 96 replies
  Sent: 14131 requests, 364499 replies (0 proxy, 0 local proxy, 25 gratuitous)
  Resolve requests rcvd: 5699
  Resolve requests dropped: 94
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 18
  Dynamic: 9, Interface: 9, Standby: 0
  Alias: 0,   Static: 0,    DHCP: 0

  IP Packet drop count for node 0/4/CPU0: 5603

  Total ARP-IDB:18
```

timers (DAGR)

To configure the Direct Attached Gateway Redundancy (DAGR) timers for sending ARP requests, use the **timers** command in DAGR peer interface configuration mode.

timers **query** *query-time* **standby** *standby-time*

Syntax Description

query *query-time*	The value is a time (in seconds) between successive ARP requests being sent out to the virtual IP address, when the group is in the query state. The range of values is 1 to 10000.
standby *standby-time*	The value is a time (in seconds) between successive ARP requests being sent out to the virtual IP address, when the group is in the standby state. The range of values is 1 to 10000.

Command Default

The default for *query-time* is 1 second, and the default for *standby-time* is 20 seconds.

Command Modes

DAGR peer interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When this function is applied, the DAGR group configuration is updated in the database. The new timer values take effect the next time the timer is set. No immediate timer restarts are triggered on the basis of this event.

Task ID

Task ID	Operations
cef	write

Examples

The following example configures a DAGR group peer with a query time of 2 and a standby time of 40:

```
Router(config-if-dagr-peer)# timers query 2 standby 40
Router(config-if-dagr-peer)#
```

DHCP Commands

This chapter describes the commands used to configure and monitor Dynamic Host Configuration Protocol (DHCP) features.

For detailed information about DHCP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

clear dhcp ipv6 relay binding

To clear DHCPv6 relay binding, use the **clear dhcp ipv6 relay binding** command in XR EXEC mode.

clear dhcp ipv6 relay binding [**client-duid** *client-duid-number*][**interface** *type interface-path-id*] [**vrf** *vrf-name*] [**location** *node-id*]

Syntax Description

client-duid *client-duid-number*	(Optional) Clears DHCPv6 relay client binding information. The argument *client-duid-number* is the client's DHCP Unique Identifier (DUID) number. **Note** Use the **show dhcp ipv6 relay binding** command to see the client DUID number.
interface *type interfac-path-id*	(Optional) Clears DHCPv6 relay client binding information for an interface. Specifies a physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
vrf *vrf-name*	(Optional) Clears DHCPv6 relay client binding information for a VPN routing and forwarding (VRF) instance.
location *node-id*	(Optional) Clears DHCPv6 relay client binding information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	execute
root-system	read, write

This example shows how to clear DHCPv6 relay binding:

```
Router# clear dhcp ipv6 relay binding
```

client-mac-mismatch

To enable DHCP MAC address verification.

client-mac-mismatch action drop

Syntax Description

action	Specifies an action for the router when the DHCP MAC address is a not a match.
drop	Drops the packet with the mismatched DHCP MAC address.

Command Default

None

Command Modes

DHCP Relay Profile Configuration Mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

Enables MAC address verification. If MAC address in the DHCPv4 protocol header does not match the L2 header source MAC address in the DHCPv4 relay profile, the frame is dropped.

Example

Use the following example to configure DHCP MAC address verification.

```
Router# configure

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile client relay
/* Enables DHCP relay profile */

Router(config-dhcpv4)# client-mac-mismatch action drop
/* Enables MAC address verification. If MAC address in the DHCPv4 protocol header does not
 match the L2 header source MAC address in the DHCPv4 relay profile,
 the frame is dropped  */

Router(config-dhcpv4-relay-profile)# commit

Router(config-dhcpv4-relay-profile)# exit
```

dhcp ipv4

To enable Dynamic Host Configuration Protocol (DHCP) for IPv4 and to enter DHCP IPv4 configuration mode, use the **dhcp ipv4** command in Global Configuration mode. To disable DHCP for IPv4 and exit the DHCP IPv4 configuration mode, use the **no** form of this command.

dhcp ipv4
no dhcp ipv4

Command Modes

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

Use the **dhcp ipv4** command to enter DHCP IPv4 configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to enable DHCP for IPv4:

```
Router# configure
Router(config)# dhcp ipv4
Router# (config-dhcpv4)#
```

dhcp ipv6

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 and to enter DHCP IPv6 configuration mode, use the **dhcp ipv6** command in XR Config mode. To disable the DHCP for IPv6, use the **no** form of this command.

dhcp ipv6

Syntax Description

This command has no keywords or arguments.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

Use the **dhcp ipv6** command to enter DHCP IPv6 configuration mode.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to enable DHCP for IPv6:

```
Router(config)# dhcp ipv6
Router(config-dhcpv6)#
```

giaddr policy

To configure how Dynamic Host Configuration Protocol (DHCP) IPv4 Relay processes BOOTREQUEST packets that already contain a nonzero giaddr attribute, use the **giaddr policy** command in DHCP IPv4 profile relay configuration submode. To restore the default giaddr policy, use the **no** form of this command.

giaddr policy {**replace** | **drop**}
no giaddr policy {**replace** | **drop**}

Syntax Description

replace	Replaces the existing giaddr value with a value that it generates.
drop	Drops the packet that has an existing nonzero giaddr value.

Command Default

DHCP IPv4 relay retains the existing nonzero giaddr value in the DHCP IPv4 packet received from a client value.

Command Modes

DHCP IPv4 profile relay configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

The **giaddr policy** command affects only the packets that are received from a DHCP IPv4 client that have a nonzero giaddr attribute.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to use the **giaddr policy** command:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile client relay
Router(config-dhcpv4-relay-profile)# giaddr policy drop
```

Related Commands

Command	Description
dhcp ipv4 , on page 115	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
helper-address, on page 119	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
profile (DHCP), on page 125	Configures a relay profile for the DHCP IPv4 component.

Command	Description
relay information, on page 127	Configures a Dynamic Host Configuration Protocol (DHCP) IPv4 relay information options in forwarded BOOTREPLY messages.

helper-address

To configure the Dynamic Host Configuration Protocol (DHCP) IPv4 relay agent to relay DHCP packets to a specific DHCP server, use the **helper-address** command in an DHCP IPv4 relay profile configuration mode. Use the **no** form of this command to clear the address.

helper-address { **vrf** *vrf-name* | *address* } **giaddr** [*gateway-address*]
no **helper-address** { **vrf** *vrf-name* | *address* } **giaddr** [*gateway-address*]

Syntax Description

vrf-name	(Optional) Specifies the name of a particular VRF.
address	IPv4 in four part, dotted decimal format.
giaddr *gateway-address*	(Optional) Specifies the gateway address to use in packets relayed to server. This keyword is applicable for IPv4 helper address.

Command Default

Helper address is not configured.

Command Modes

DHCP IPv4 relay profile configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

A maximum of upto eight helper addresses can be configured.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to set the helper-address for a VRF using the **helper address** command in DHCP IPv4 relay profile class configuration mode:

```
RP/0/CPU0:router(config)#  dhcp ipv4
RP/0/CPU0:router(config-dhcpv4)# profile profile1 relay
RP/0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf my-server-vrf 192.0.2.1
```

Related Commands

Command	Description
dhcp ipv4	Enables Dynamic Host Configuration Protocol (DHCP) for IPv4 and enters DHCP IPv4 configuration mode.
relay information check	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.

Command	Description
relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.

helper-address (ipv6)

To configure the Dynamic Host Configuration Protocol (DHCP) IPv6 relay agent for prefix delegation to relay DHCP packets to a specific DHCP server, use the **helper-address** command in the DHCP IPv6 profile configuration submode. Use the **no** form of this command to clear the address.

helper-address *ipv6-address* | **vrf** *vrf-address* [**interface** *type* *interface-path-id*]
no helper-address *ipv6-address* | **vrf** *vrf-address* [**interface** *type* *interface-path-id*]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
interface *type*	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between value s is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

DHCP IPv6 profile configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read, write

Example

This is a sample output that shows how to set the helper-address using the **helper-address** command

```
Router# config
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile p1 relay
Router(config-dhcpv6-profile)# helper-address 2001:DB8::1 HundredGigE 0/2/0/0
```

Related Commands

Command	Description
dhcp ipv6, on page 116	Enables Dynamic Host Configuration Protocol (DHCP) for IPv6.

hop-count-seed

To configure the hop-count in relay-forward message for a DHCP relay agent as zero, use the `hop-count-seed` command in the DHCP IPv6 configuration mode. By default, hop-count in relay-forward message for DHCP relay agents is set to one.

hop-count-seed
no hop-count-seed

Syntax Description

This command has no keywords or arguments.

Command Default

If this command is not configured, by default, hop-count in relay-forward message for DHCP relay agents is set to one.

Command Modes

DHCP IPv6 configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

Use this command only on routers that are configured as DHCP relay agents. You can only configure this command in the DHCP IPv6 mode and not on DHCP IPv4 mode.

Task ID

Task ID	Operations
ip-services	read, write

The following is an example of the **hop-seed-count** command:

```
Router# config
Router(config)# dhcp ipv6
Router(dhcp-ipv6)# hop-count-seed
```

iana-route-add

To enable route addition for identity association for non-temporary address (IANA), use the **iana-route-add** command in DHCPv6 relay profile configuration submode. To disable route addition to IANA, use the **no** form of this command.

iana-route-add
no iana-route-add

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled.

Command Modes

DHCP IPv6 relay profile configuration submode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

The DHCPv6 relay is capable of installing routes for multiple identity association for prefix delegation (IAPD) options within a DHCPv6 message. The route addition for IAPD is enabled by default. The DHCPv6 relay is capable of installing routes for IANA as well, but this feature is disabled by default. Users can enable the route addition to IANA feature by using **iana-route-add** command in DHCPv6 relay profile configuration submode.

Task ID

Task ID	Operation
ip-services	read, write

Example

This example shows how to enable route addition to IANA:

```
Router# config
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile client relay
Router(config-dhcpv6-relay-profile)# iana-route-add
```

profile (DHCP)

To configure a DHCP relay profile, use the **profile** command in DHCP IPv4 or DHCP IPv6 configuration mode. To disable this feature and exit the profile mode, use the **no** form of this command.

profile *name* **relay**
no profile *name* **relay**

Syntax Description

name	Name that uniquely identifies the relay or snoop profile.
relay	Configures a DHCP relay profile. A DHCP relay agent is a host that forwards DHCP packets between clients and servers. When the clients and servers are not on the same physical subnet, the relay agents are used to forward requests and replies between them. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks rather transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway IP address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

Command Default

None

Command Modes

DHCP IPv4 configuration

DHCP IPv6 configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

This example shows how to use the **profile** command to configure DHCP IPv6 relay profile:

```
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile TEST relay
Router(config-dhcpv6-relay-profile)#
```

This example shows how to use the **profile** command to configure DHCP IPv4 relay profile:

```
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile TEST relay
Router(config-dhcpv4-relay-profile)#
```

relay information

To configure Dynamic Host Configuration Protocol (DHCP) IPv4 relay information options, use the relay information command in DHCP IPv4 relay profile configuration submode. To restore the default relay information policy, use the no form of this command.

relay information { **check** | **option** [**allow-untrusted** | **remote-id format-type** { **ascii** *ascii-value* | **hex** *hex-value* } | **subscriber-id** *subscriber-value* | **vpn** | **vpn-mode** { **cisco** | **rfc** }] | **policy** { **drop** | **encapsulate** | **keep** } }
no relay information { **check** | **option** [**allow-untrusted** | **remote-id format-type** { **ascii** *ascii-value* | **hex** *hex-value* } | **subscriber-id** *subscriber-value* | **vpn** | **vpn-mode** { **cisco** | **rfc** }] | **policy** { **drop** | **encapsulate** | **keep** } }

Syntax Description

check	Validates the relay agent information option in forwarded BOOTREPLY messages.
option	Configures relay agent information options in forwarded BOOTREQUEST messages.
allow-untrusted	Forwards untrusted packets.
remote-id format-type	Configures the value of the remote-id in either ascii or hex format.
subscriber-id *subscriber-value*	Configures the value of the subscriber-id
vpn	Configures VPN suboptions in forwarded BOOTREQUEST messages.
vpn-mode	Configures VPN suboptions mode either in CISCO proprietary or RFC compliance.
policy	Configures relay agent information option policy
drop	Directs the DHCP IPv4 Relay to discard BOOTREQUEST packets with the existing relay information option
keep	Directs the DHCP IPv4 Relay not to discard a BOOTREQUEST packet that is received with an existing relay information option and to keep the existing relay information option value.
encapsulate	Encapsulates the DHCP relay agent information option received from a prior relay agent in forwarded BOOTREQUEST messages.

Command Default

The DHCP IPv4 Relay does not discard a BOOTREQUEST packet that has an existing relay information option. The option and the existing relay information option value is replaced.

Command Modes

DHCP IPv4 relay profile configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

The encapsulate keyword allows the second relay agent to encapsulate option 82 information in a message received from the first relay agent, if it is also configured to add its own option 82 information. This configuration allows the DHCP server to use option 82 information from both relay agents.

Task ID

Task ID	Operation
ip-services	read, write
basic-services	read, write

This is sample output from executing the relay information policy command:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile TEST relay
Router(config-dhcpv4-relay-profile)# relay information policy keep
```

This example shows how to encapsulate the DHCP relay agent information option:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile TEST relay
Router(config-dhcpv4-relay-profile)# relay information policy encapsulate
```

Related Commands

Command	Description
dhcp ipv4	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
helper-address	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information check	Configures a DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
relay information option	Enables the system to insert a DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.
relay information option allow-untrusted	Configures the DHCP component to not drop BOOTREQUEST messages that have the relay information option set and the giaddr set to zero.

show dhcp ipv4 relay

To display the Dynamic Host Configuration Protocol (DHCP) IPv4 relay agent packet information, use the **show dhcp ipv4 relay** command in the XR EXEC mode.

show dhcp ipv4 relay { **profile** [**name** *profile-name*] | **statistics** [**detail**] } [**location** *node-id*]

Syntax Description

profile name *profile-name*	(Optional) Displays the profile name.
statistics	(Optional) Displays the profile statistics.
location *node-id*	(Optional) Displays the information for the specified node.

Command Default

No default behavior or values

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv4 relay statistics** command when none of the optional keywords or arguments are used command:

```
Router# show dhcp ipv4 relay statistics

                  Bridge              |       RX        |       TX        |        DR       |
-------------------------------------------------------------------------------------------------
 default                              |            0    |            0    |            0    |
```

The following is sample output from the **show dhcp ipv4 relay profile** command:

```
Router# show dhcp ipv4 relay profile
DHCP IPv4 Relay Profiles
--------------------------
r1
r2
```

The following is sample output from the **show dhcp ipv4 relay profile name** *profile-name* command:

```
Router# show dhcp ipv4 relay profile name R1
DHCP IPv4 Relay Profile R1:

Helper Addresses:
10.10.10.1, vrf default
Information Option: Disabled
Information Option Allow Untrusted: Disabled
Information Option Policy: Replace
Information Option Check: Disabled
Giaddr Policy: Keep
Broadcast-flag Policy: Ignore

VRF References:
default
Interface References:
FINT0_RP0_CPU0
MgmtEth0_RP0_CPU0_0
```

show dhcp ipv6 relay binding

To display DHCPv6 client bindings for relay, use the **show dhcp ipv6 relay binding** command in XR EXEC mode.

show dhcp ipv6 relay binding [**client-duid** *client-duid-number*] [[**detail**]] | [[**interface** *type* *interface-path-id*]] | [[**location** *node-id*]] | [[**summary**]] | [**vrf** *vrf-name*]

Syntax Description

client-duid *client-duid-number*	(Optional) Displays DHCPv6 relay client binding information. The argument *client-duid-number* is the client's DHCP Unique Identifier (DUID) number. **Note** Use the **show dhcp ipv6 relay binding** command to see the client DUID number.
detail	(Optional) Displays detailed DHCPv6 relay client binding information for all clients.
interface *type* *interfac-path-id*	(Optional) Displays DHCPv6 relay client binding by interface. Specifies a physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
location *node-id*	(Optional) Displays detailed DHCPv6 relay client binding information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays the summary of DHCPv6 relay client binding.
vrf *vrf-name*	(Optional) Displays DHCPv6 relay client binding information for a VPN routing and forwarding (VRF) instance.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

This is the sample output for show dhcp ipv6 relay binding command:

```
Router# show dhcp ipv6 relay binding
Summary:
Total number of clients: 1

IPv6 Address: fc00:35:0:ef5c:a932:239f:1b0e:e4ed/128 (BVI3500)
    Client DUID: 000100011b626e6f0000cae2da26
    IAID: 0x0
    VRF: default
    Lifetime: 172800 secs (2d00h)
    Expiration: 172766 secs (1d23h)
```

show dhcp ipv6 relay statistics

To display DHCPv6 relay statistics, use the **show dhcp ipv6 relay statistics** command in XR EXEC mode.

show dhcp ipv6 relay statistics [**vrf** *vrf-name*] | [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays DHCPv6 relay statistics information in details.
location *node-id*	(Optional) Displays DHCPv6 relay debug statistics information for for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
vrf *vrf-name*	(Optional) Displays DHCPv6 relay statistics information for a VPN routing and forwarding (VRF) instance.
location *node-id*	(Optional) Displays detailed DHCPv6 relay statistics information for a specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

This is the sample output for **show dhcp ipv6 relay statistics** command:

```
Router# show dhcp ipv6 relay statistics
                  VRF                     |       RX        |       TX        |        DR
|
-------------------------------------------------------------------------------------------
default                                  |          241   |            5   |          236   |
**nVSatellite                            |           0  |           0  |           0  |
red4                                     |           0  |           0  |           0  |
red6                                     |           0  |           0  |           0  |
**eint                                   |           0  |           0  |           0  |
```

vrf (relay profile)

To configure a relay profile on a VPN routing and forwarding (VRF) instance, use the **vrf (relay profile)** command in Dynamic Host Configuration Protocol (DHCP) IPv4 configuration mode. To disable this feature, use the **no** form of this command.

vrf { *vrf-name* | **default** | **all** } **relay** [**profile** *profile-name*]
no vrf { *vrf-name* | **default** | **all** } **relay** [**profile** *profile-name*]

Syntax Description

vrf-name	User-defined name for the VRF.
default	Specifies a profile for the default VRF.
all	Specifies a profile for all VRFs.
relay	Specifies a relay profile.
profile *profile-name*	Specifies a name for the profile.

Command Default

If **default** is selected, then the configuration defaults to VRF.

Command Modes

DHCP IPv4 configuration

Command History

Release	Modification
Release 7.2.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the relay profile for all VRFs:

```
Router# config
Router(config)# dhcp ipv4
Router(config-dhcpv4)# vrf all
```

Related Commands

Command	Description
dhcp ipv4 , on page 115	Enables DHCP for IPv4 and enters DHCP IPv4 configuration mode.
giaddr policy, on page 117	Configures how a relay agent processes BOOTREQUEST messages that already contain a nonzero giaddr attribute.

Command	Description
helper-address, on page 119	Configures the DHCP relay agent to relay packets to a specific DHCP Server.
relay information, on page 127	Configures a Dynamic Host Configuration Protocol (DHCP) IPv4 relay information options in forwarded BOOTREPLY messages.

Cisco Express Forwarding Commands

This chapter describes the commands used to configure and monitor Cisco Express Forwarding (CEF) on a Cisco 8000 Series Router.

For detailed information about ACL concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Command Reference for Cisco 8000 Series Routers*

cef adjacency route override rib

To enable the CEF prefer Routing Information Base (RIB) prefixes over Adjacency Information Base (AIB) prefixes in the Global configuration mode. To enable the CEF prefer AIB prefixes over RIB prefixes, use the **no** form of this command.

cef adjacency route override rib

no cef adjacency route override rib

Syntax Description

route	Enables adjacency route configuration .
override	Sets override options for the adjacency routes.
rib	Sets options for adjacency routes to override the RIB routes.

Command Default

By default, CEF prefers RIB prefixes over AIB prefixes.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

CEF may prefer the L2 adjacency for forwarding over the RIB (routing) entry under the following conditions:

- When there is no local ARP entry (yet).

  ARP learning may result in the router creating a forwarding entry.

- A forwarding entry of /32 (or /128 for IPv6) RIB routes are overridden when there is a covering connected or attached route.

  If an interface has a larger subnet, and you want to redirect a /32 out of that subnet of a different interface via a static route.

To deviate from the behavior of preferring a L2 adjacency for forwarding over a route entry, use the **cef adjacency route override rib** command.

Task ID

Task ID	Operation
cef	read, write

Example

The following example shows how to override the CEF adjacency route:

```
Router# configure
Router# cef adjacency route override rib
```

cef load-balancing

To configure load-balancing parameters, use the **cef load-balancing** command in Global configuration mode. To enable the default CEF load-balancing behavior, use the **no** form of this command.

cef load-balancing { **mode hierarchical** { **ucmp group-size** | **ecmp min-path** } <*range*> | **recursive oor mode dampening-and-dlb** [**dampening resource-threshold** <*percentage*> | **dlb resource-threshold** <*percentage*> | **max-duration** <*secs*>] }

Syntax Description

mode	Specifies the mode as hierarchical.
hierarchical	Specifies the configuration for multi-level load balancing in CEF.
ucmp	Specifies the **ucmp** parameters for CEF load-balancing configuration.
group-size	Enables **ucmp** group size for hierarchical load balancing (HLB).
ecmp	Specifies the **ecmp** parameters for CEF load-balancing configuration.
min-path	Specifies the minimum number of paths required for hierarchical **ecmp** load balancing.
range	Specifies the range of values for configuring the group size for **ucmp** and minimum paths for **ecmp** in hierarchical load balancing. The routers supports the values ranging from 1 to 128.
recursive	Enables recursive route configuration.
oor	Enables oor configuration.
dlb	Specifies the dynamic load balancing (DLB) parameter in CEF load balancing.
dampening-and-dlb	Enables dampening and dlb mode for oor handling.
dampening	Configure dampening mode parameters.
resource-threshold	Specifies the resource threshold percentage to enable dynamic load-balancing mode.
percentage	Specifies the threshold percentage for enabling FIB dampening and DLB features.
max-duration	Specifies the maximum duration time configuration for dampening and dynamic load balancing in CEF load balancing.
secs	Specifies the maximum duration time, in seconds, for configuring dampening and dynamic load balancing in CEF load balancing. You can configure the time range from 1 to 600 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 24.2.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **cef load-balancing mode hierarchical ecmp min-paths** command is a replacement for the **cef hierarchical-load-balancing ecmp min-paths** command.

If the number of paths exceeds 128, HLB is automatically applied.

The **cef load-balancing mode hierarchical ucmp group-size** command is a replacement for the **cef hierarchical-load-balancing ucmp group-size** command.

Task ID

Task ID	Operation
cef	read, write

Example

The following example shows how to enable FIB dampening and DLB features with default values of dampening threshold percentage and max switchover duration and dlb threhold percentage as (70%, 300 sec, 90%)

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# cef load-balancing recursive oor mode dampening-and-dlb
```

The following example shows how to enable FIB dampening and DLB features with default values of dampening threshold percetange and max switchover duration and dlb threhold percentage as (70%, 90%).

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# cef load-balancing recursive oor mode dampening-and-dlb max-duration
 600
```

The following example shows how to configure dampening and dynamic load balancing with specified resource-threshold for dampening and dlb each and maximum duration for switchover time.

Note The dampening threshold value should be lower than the DLB threshold.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# cef load-balancing recursive oor mode dampening-and-dlb dampening
resource-threshold 99 max-duration 600 dlb resource-threshold 99
```

The following example shows how to configure the group size for ucmp in hierarchical load balancing

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# cef load-balancing mode  hierarchical ucmp group-size 128
```

The following example shows how to configure the minimum paths for hierarchical ecmp load balancing.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# cef load-balancing mode  hierarchical ecmp min-path 128
```

clear adjacency statistics

To clear adjacency packet and byte counter statistics, use the **clear adjacency statistics** command in XR EXEC mode.

clear adjacency statistics [**ipv4** [**nexthop** *ipv4-address*] | **mpls** | **ipv6**] [*interface-type interface-instance* | **location** *node-id*]

Syntax Description

ipv4	(Optional) Clears only IPv4 adjacency packet and byte counter statistics.
nexthop *ipv4-address*	(Optional) Clears adjacency statistics that are destined to the specified IPv4 nexthop.
mpls	(Optional) Clears only MPLS adjacency statistics.
ipv6	(Optional) Clears only IPv6 adjacency statistics.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-instance	(Optional) Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface MgmtEth0/ RP0 • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Clears detailed adjacency statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **clear adjacency statistics** command is useful for troubleshooting network connection and forwarding problems.

If you do not specify any of the optional keywords, all adjacency statistics are cleared for the node on which the command is issued.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Related Commands

Command	Description
show adjacency, on page 157	Displays the IPv4 CEF adjacency table.

clear cef ipv4 drops

To clear Cisco Express Forwarding (CEF) IPv4 packet drop counters, use the **clear cef ipv4 drops**command in XR EXEC mode.

clear cef ipv4 drops location *node-id*

Syntax Description

location *node-id*	Clears IPv4 packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command will clear IPv4 CEF drop counters only for the node on which the command is issued.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv4 Cisco Express Forwarding (CEF) table packet drop counters, and clears IPv4 CEF drop counters for location 0/RP0/CPU0:

```
Router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :               0
  No route drops       packets :               0
  No Adjacency drops   packets :               0
  Checksum error drops packets :               0
  RPF drops            packets :               0
  RPF suppressed drops packets :               0
  RP destined drops    packets :               0
  Discard drops        packets :               0
  GRE lookup drops     packets :               0
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :               0
  LISP decap err drops packets :               0

Node: 0/RP1/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :               0
  No route drops       packets :               0
  No Adjacency drops   packets :               0
  Checksum error drops packets :               0
  RPF drops            packets :               0
  RPF suppressed drops packets :               0
  RP destined drops    packets :               0
  Discard drops        packets :               0
  GRE lookup drops     packets :               0
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :               0
  LISP decap err drops packets :               0

Router# clear cef ipv4 drops location 0/RP0/CPU0

  Node: 0/RP0/CPU0
  Clearing CEF Drop Statistics
```

clear cef ipv4 exceptions

To clear IPv4 Cisco Express Forwarding (CEF) exception packet counters, use the **clear cef ipv4 exceptions** command in XR EXEC mode mode.

clear cef ipv4 exceptions location *node-id*

Syntax Description

location *node-id*	Clears IPv4 CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command will clear IPv4 CEF exception packet counters for all nodes.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv4 Cisco Express Forwarding (CEF) exception packet counters, and clear s IPv4 CEF exception packets node 0/RP0/CPU0:

```
Router# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :              0
  Unsupported packets :              0
  Redirect    packets :              0
  Receive     packets :              0
  Broadcast   packets :              0
  IP options  packets :              0
  TTL expired packets :              0
  Fragmented  packets :              0
Node: 0/RP1/CPU0
  Slow encap  packets :              3
  Unsupported packets :              0
  Redirect    packets :              0
  Receive     packets :          12787
  Broadcast   packets :          74814
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0

Router# clear cef ipv4 exceptions location 0/RP0/CPU0

Node: 0/RP0/CPU0
Clearing CEF Exception Statistics
```

clear cef ipv6 drops

To clear Cisco Express Forwarding (CEF) IPv6 packet drop counters, use the **clear cef ipv6 drop** command in XR EXEC mode.

clear cef ipv6 drops location *node-id*

Syntax Description

location *node-id*	Clears IPv6 packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command clears IPv6 CEF drop counters for all nodes.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv6 Cisco Express Forwarding (CEF) table packet drop counters, and clears IPv6 CEF drop counters for location 0/RP0/CPU0:

```
Router# show cef ipv6 drops

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :               0
  No route drops       packets :               1
  No Adjacency drops   packets :               0
  Checksum error drops packets :               0
  RPF drops            packets :               0
  RPF suppressed drops packets :               0
  RP destined drops    packets :               0
  Discard drops        packets :               0
  GRE lookup drops     packets :               0
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :               0
  LISP decap err drops packets :               0

Node: 0/RP1/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :               0
  No route drops       packets :               1
  No Adjacency drops   packets :               0
  Checksum error drops packets :               0
  RPF drops            packets :               0
  RPF suppressed drops packets :               0
  RP destined drops    packets :               0
  Discard drops        packets :               0
  GRE lookup drops     packets :               0
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :               0
  LISP decap err drops packets :               0

Router# clear cef ipv6 drop

Node: 0/RP0/CPU0
Clearing CEF Drop Statistics
```

clear cef ipv6 exceptions

To clear IPv6 Cisco Express Forwarding (CEF) exception packet counters, use the **clear cef ipv6 exceptions** command in XR EXEC mode .

clear cef ipv6 exceptions location *node-id*

Syntax Description

location *node-id*	Clears IPv6 CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command clears IPv6 CEF exception packet counters for all nodes.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Examples

The following example displays sample output for the IPv6 Cisco Express Forwarding (CEF) exception packet counters, and clears the IPv6 CEF exception packets for location:

```
Router# show cef ipv6 exceptions

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :              0
  Unsupported packets :              0
  Redirect    packets :              0
  Receive     packets :              1
  Broadcast   packets :              0
  IP options  packets :              0
  TTL expired packets :              0
  Fragmented  packets :              0

Node: 0/RP1/CPU0
  Slow encap  packets :              0
  Unsupported packets :              0
  Redirect    packets :              0
  Receive     packets :              7
  Broadcast   packets :              0
  IP options  packets :              0
  TTL expired packets :              0
  Fragmented  packets :              0

Router# clear cef ipv6 exceptions location 0/RP0/CPU0

Node: 0/RP0/CPU0
Clearing CEF Exception Statistics
```

hw-module profile cef

To configure cef profile on a Global Configuration level, use the hw-module profile cef command in the XR Config mode.

Note Use the **lpts acl** option in the hw-module profile cef command in the Global Configuration mode. To disable the LPTS ACL mode, use the **no** form of this command.

hw-module profile cef { [**bgplu enable**] | [**dark-bw enable**] | [**lpts acl**] | [**source-rtbh enable**] }

Syntax Description

bgplu	Configures the bgplu feature.
dark-bw	Configures the dark bandwidth.
lpts acl	Configures the lpts acl mode
source-rtbh enable	Configures source-based Remote Triggered Black Hole filtering (RTBH).

Command Default

No default behavior or values

Command Modes

XR Config

Command History

Release	Modification
Release 7.5.2	The **lpts acl** option was introduced.
Release 7.0.12	This command was introduced.
Release 24.2.1	This command was modified. The **source-rtbh enable** keyword-pair was introduced.

Task ID

Task ID	Operations
basic-services	read, write
cef	read, write

Usage Guidelines

You must reload the router after executing the **hw-module profile cef** command.

For more information about configuring Dark Bandwidth (dark-bw), see chapter *Implementing MPLS Traffic Engineering* in the *MPLS Configuration Guide for Cisco 8000 Series Routers*.

hw-module profile route scale

To increase the route scale for IPv4 or IPv6 traffic types, use the **hw-module profile stats route-scale** command in XR Config mode.

hw-module profile route scale lpm tcam-banks wide-entries shortened

Syntax Description

lpm tcam-banks	Increases the IPv4 route scale from 2 million to 3 million entries and IPv6 route scale from 0.5 million to 1 million entries.
lpm wide-entries shortened	Shortens the wide routing prefixes for IPv6 addresses.

Command Default

By default, the route scale for IPv4 traffic is 2 million entries and IPv6 traffic is 0.5 million entries.

Command Mode

XR Config

Command History

Release	Modification
Release 24.1.1	The **lpm wide-entries shortened** keyword was introduced.
Release 7.9.1	This command was introduced.

Usage Guidelines

- You must reload the router after executing the **hw-module profile route scale** command.
- When you increase the route scale, it will result in restricted resources for packet classification features such as Security ACL, QoS ACL, BGP Flowspec, and LPTS.
- The **hw-module profile route scale lpm wide-entries shortened** command isn't enabled by default, and we recommend using it judiciously to accomodate higher number of wide-entry IPv6 prefixes.

Task ID	Operations
config-services	read, write
root-lr	read, write

Examples

The following example shows you how to configure the **hw-module profile route scale** command:

```
Router# config
Router(config)# hw-module profile route scale lpm tcam-banks
Router(config)# commit
Router# reload location all
```

The following example shows you how to configure the **hw-module profile route scale lpm wide-entries shortened** command:

```
Router# config
Router(config)# hw-module profile route scale lpm wide-entries shortened
Router(config)# commit
Router# reload location all
```

show adjacency

To display Cisco Express Forwarding (CEF) adjacency table information, use the **show adjacency** command in XR EXEC mode.

show adjacency [**ipv4** [**nexthop** *ipv4-address*] | **mpls** | **ipv6**] [*interface type interface-instance*] [**remote**] [**detail**] [**location** *node-id*]

Syntax Description

ipv4	(Optional) Displays only IPv4 adjacencies.
nexthop *ipv4-address*	(Optional) Displays adjacencies that are destined to the specified IPv4 nexthop.
mpls	(Optional) Displays only MPLS adjacencies.
ipv6	(Optional) Displays only IPv6 adjacencies.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-instance	Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
remote	(Optional) Displays only remote adjacencies. A remote adjacency is an internal adjacency used to forward packets between line cards.
detail	(Optional) Displays detailed adjacency information, including Layer 2 information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command is used to verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF adjacency table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from **show adjacency** command with the **location** keyword specified:

```
Router# show adjacency location 0/RP1/CPU0

Interface                   Address                  Version  Refcount Protocol
FH0/0/0/21                  (interface)                    5        1(    0)
FH0/0/0/17                  (interface)                    9        1(    0)
Mg0/RP0/CPU0/0              (interface)                    1        1(    0)
FH0/0/0/13                  (interface)                   13        1(    0)
Hu0/0/0/34                  (interface)                   27        1(    0)
FH0/0/0/3                   (interface)                   23        1(    0)
Hu0/0/0/30                  (interface)                   31        1(    0)
FH0/0/0/7                   (interface)                   19        1(    0)
Hu0/0/0/26                  (interface)                   35        1(    0)
FH0/0/0/11                  (interface)                   15        1(    0)
FH0/0/0/20                  (interface)                    6        1(    0)
FH0/0/0/16                  (interface)                   10        1(    0)
FH0/0/0/12                  (interface)                   14        1(    0)
Hu0/0/0/33                  (interface)                   28        1(    0)
FH0/0/0/4                   (interface)                   22        1(    0)
Hu0/0/0/29                  (interface)                   32        1(    0)
FH0/0/0/8                   (interface)                   18        1(    0)
Hu0/0/0/25                  (interface)                   36        1(    0)
Hu0/0/0/24                  (interface)                   37        1(    0)
FH0/0/0/23                  (interface)                    3        1(    0)
FH0/0/0/19                  (interface)                    7        1(    0)
Hu0/0/0/32                  (interface)                   29        1(    0)
FH0/0/0/15                  (interface)                   11        1(    0)
Hu0/0/0/28                  (interface)                   33        1(    0)
FH0/0/0/1                   (interface)                   25        1(    0)
FH0/0/0/5                   (interface)                   21        1(    0)
FH0/0/0/9                   (interface)                   17        1(    0)
FH0/0/0/0                   (interface)                    2        1(    0)
FH0/0/0/22                  (interface)                    4        1(    0)
FH0/0/0/18                  (interface)                    8        1(    0)
FH0/0/0/14                  (interface)                   12        1(    0)
Hu0/0/0/35                  (interface)                   26        1(    0)
FH0/0/0/2                   (interface)                   24        1(    0)
Hu0/0/0/31                  (interface)                   30        1(    0)
FH0/0/0/6                   (interface)                   20        1(    0)
Hu0/0/0/27                  (interface)                   34        1(    0)
FH0/0/0/10                  (interface)                   16        1(    0)
```

This table describes the significant fields shown in the display.

Table 7: show adjacency Command Field Descriptions

Field	Description
Interface	Outgoing interface associated with the adjacency.
Address	Address can represent one of these addresses: • Next hop IPv4 or IPv6 address • Point-to-Point address Information in parentheses indicates different types of adjacency.
Version	Version number of the adjacency. Updated whenever the adjacency is updated.
Refcount	Number of references to this adjacency.
Protocol	Protocol for which the adjacency is associated.
0f000800 and 000c86f33d330800453a21c10800	Layer 2 encapsulation string.
mtu	Value of the maximum transmission unit (MTU).
flags	Internal field.
packets	Number of packets going through the adjacency.
bytes	Number of bytes going through the adjacency.

show cef bgp-attribute

To display Border Gateway Protocol (BGP) attributes for Cisco Express Forwarding (CEF), use the **show cef bgp-attribute** command in XR EXEC mode.

show cef bgp-attribute [**attribute-id index-id**] [**local-attribute-id index-id**] [**location** *node-id*]

Syntax Description

attribute-id *index-id*	(Optional) Displays FIB attribute index.
local-attribute-id *index-id*	(Optional) Displays FIB local attribute index.
location *node-id*	(Optional) Displays BGP information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The default location is active RP.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
cef	read

Examples

The following example shows how to use the **show cef bgp-attribute** command:

```
Router# show cef bgp-attribute

Total number of entries: 75742
BGP Attribute ID: 0x2058a, Local Attribute ID: 0x1
    Origin AS:    195, Next Hop AS:        195
BGP Attribute ID: 0x20583, Local Attribute ID: 0x2
    Origin AS:    22, Next Hop AS:        22
BGP Attribute ID: 0x20582, Local Attribute ID: 0x3
    Origin AS:    21, Next Hop AS:        21
BGP Attribute ID: 0x20585, Local Attribute ID: 0x4
    Origin AS:    28, Next Hop AS:        28
BGP Attribute ID: 0x20584, Local Attribute ID: 0x5
    Origin AS:    27, Next Hop AS:        27
BGP Attribute ID: 0x2057f, Local Attribute ID: 0x6
    Origin AS:    86, Next Hop AS:        86
BGP Attribute ID: 0x2058b, Local Attribute ID: 0x7
    Origin AS:    196, Next Hop AS:        196
BGP Attribute ID: 0x20589, Local Attribute ID: 0x8
    Origin AS:    194, Next Hop AS:        194
```

This table describes the significant fields shown in the display.

Table 8: show cef bgp-attribute Command Field Descriptions

Field	Description
BGP Attribute ID	Displays the id assigned by BGP.
Local Attribute ID	Displays the id assigned by FIB.
Origin AS	Displays the origin AS of the prefix that carries this attribute id.
Next Hop AS	Displays the AS that contains the BGP nexthop for this prefix.

show cef

To display information about packets forwarded by Cisco Express Forwarding (CEF), use the **show cef** command in XR EXEC mode.

show **cef** [*prefix* [*mask*]] [**hardware** {**egress**} | **detail**] [**location** {*node-id* | **all**}]

Syntax Description

prefix	(Optional) Longest matching CEF entry for the specified IPv4 destination prefix.
mask	(Optional) Exact CEF entry for the specified IPv4 prefix and mask.
hardware	(Optional) Displays detailed information about hardware.
egress	Displays information from the egress packets.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	(Optional) Displays all locations.

Command Default

When the prefix is not explicitly specified, this command displays all the IPv4 prefixes that are present in CEF. When not specified, the location defaults to the active Route Processor (RP) node.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output shows the load information flag from the **show cef** command for both **hardware** and **ingress** keywords:

```
Router# show cef 192.0.2.1/16 hardware ingress location 0/RP0/CPU0

Tue Apr 28 04:17:05.105 UTC
192.0.2.1/32, version 25, internal 0x1000001 0x0 (ptr 0x8e7cf528) [1], 0x0 (0x8e9a7a68),
0x0 (0x0)
 Updated Apr 28 04:06:38.879
 local adjacency 9.1.58.5
```

```
Prefix Len 32, traffic index 0, precedence n/a, priority 1
 gateway array (0x8e80fe90) reference count 2, flags 0x0, source rib (7), 0 backups
               [3 type 3 flags 0x8401 (0x8e8c1cd8) ext 0x0 (0x0)]
 LW-LDI[type=3, refc=1, ptr=0x8e9a7a68, sh-ldi=0x8e8c1cd8]
 gateway array update type-time 1 Apr 28 04:06:38.879
LDI Update time Apr 28 04:06:38.899
LW-LDI-TS Apr 28 04:06:38.899
  via 192.0.10.1/32, Bundle-Ether4, 7 dependencies, weight 0, class 0 [flags 0x0]
   path-idx 0 NHID 0x0 [0x8fa2a260 0x0]
   next hop 9.1.58.5/32
   local adjacency
  via 192.0.20.1/32, Bundle-Ether28, 7 dependencies, weight 0, class 0 [flags 0x0]
   path-idx 1 NHID 0x0 [0x8fa2a140 0x0]
   next hop 9.9.28.2/32
   local adjacency
  via 10.28.1.2/32, Bundle-Ether2801, 7 dependencies, weight 0, class 0 [flags 0x0]
   path-idx 2 NHID 0x0 [0x8fa2a1d0 0x0]
   next hop 192.0.30.1/32
   local adjacency

   Load distribution: 0 1 2 (refcount 3)

   Hash  OK  Interface                 Address
   0     Y   Bundle-Ether4             192.0.10.1
   1     Y   Bundle-Ether28            192.0.20.1
   2     Y   Bundle-Ether2801          192.0.30.1
```

show cef exact-route (user-data)

To display the route taken from a source IP to a destination IP , use the **show cef exact-route** command in XR EXEC mode.

show cef [**exact-route** *ipv4-source-address* *ipv4-destination-address* **protocol** *protocol* **source-port** *source-port* **destination-port** *destination-port* { **ingress-interface** *ingress-interface* | **user-data** *user-data* **ingress-interface** *ingress-interface* [**brief** | **detail** | **hardware** | **internal** | **location** | **policy-class** | **protocol**] }]

Syntax Description

exact-route	(Optional) Displays the egress interface where traffic corresponding to the other specified parameters will be sent.
ipv4-source-address	Specifies IPv4 source address in x.x.x.x format.
ipv4-destination-address	Specifies IPv4 destination address in x.x.x.x format.
protocol *protocol*	Specifies protocol number or name for this route. For more information, use the question mark (?) online help function.
source-port *source-port*	Specifies the source port number. The range is from 0 to 65535.
destination-port *destination-port*	Specifies the destination port number. The range is from 0 to 65535.
ingress-interface	(Optional) Specifies the ingress interface information.
user-data *user-data*	(Optional) Specifies the additional user chosen data bytes used in multi-path computation. In *user-data*, you can enter 1-4 bytes in hexadecimal.
ingress-interface *ingress-interface*	Specifies the ingress interface information.
brief	(Optional) Displays brief information of CEF table.
detail	(Optional) Displays full information of CEF table.
hardware	(Optional) Displays information from hardware.
location	(Optional) Provides the forwarding information for the designated node. The node-id argument is entered in the *rack/slot/module* notation.
policy-class	(Optional) Class for policy-based tunnel selection.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.5	The keyword **user-data** was introduced.

Release	Modification
Release 24.2.11	The keyword **user-data** was introduced.
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF table on the node in which the command is issued. Otherwise, the command is effective on the node specified by the **location** *node-id* keyword and argument.

Task ID

Task ID	Operations
cef	read

Examples

The following is a sample output of the **show cef exact-route** command:

```
Router# show cef exact-route 100.0.0.10 60.1.0.1 protocol 253 source-port 0 destination-port
 0 user-data 0x4 ingress-interface HundredGigE0/0/0/2 location 0/0/cpu0

Mon Aug 14 07:56:18.145 UTC

Unsupported protocol value 253
48.0.0.0/4, version 1377, internal 0x1000001 0x20 (ptr 0x8b470510) [1], 0x400 (0x8e0d45e8),
 0x0 (0x0)
 Updated Aug 14 07:50:20.022
 local adjacency to HundredGigE0/0/0/26.29

 Prefix Len 4, traffic index 0, precedence n/a, priority 2
   via HundredGigE0/0/0/26.29
   via 34.0.9.2/32, HundredGigE0/0/0/26.29, 5 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 1 NHID 0x0 [0x8c60c480 0x0]
    next hop 34.0.9.2/32
    local adjacency
```

show cef ext-client

To display Cisco Express Forwarding (CEF) external client dependency information, use the**show cef ext-client** command in XR EXEC mode.

show cef ext-client [**detail** | **hardware** | **internal** | **location** | **summary**]

Syntax Description

detail	(Optional) Displays all information of all external clients in details.
hardware	(Optional) Displays hardware information of external clients.
internal	(Optional) Displays internal information of external clients.
location *node-id*	(Optional) Displays external client dependency information for the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
prefix	(Optional) Displays external client information for a specific prefix.
resolved	(Optional) Displays external client information for resolved ECD prefixes.
summary	(Optional) Displays summary of external client information.
unresolved	(Optional) Displays external client information for unresolved specific prefixes.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

The following sample output is from the show cef external command:

```
Router#show cef ext-client summary
Thu Apr  9 15:33:32.259 UTC
Client Name: mfwd6 (comp-id: 0x89a)
------------
Protocol            : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
```

```
ECD version: 1
# of ECD Pathlist: 0

Client Name: l2fib_mgr (comp-id: 0x7e6d)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0

Client Name: ipv4_IPV4_MRIB (comp-id: 0x305)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0

Client Name: XTC_AGENT (comp-id: 0x19fc)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0

Client Name: object_tracking (comp-id: 0xc99)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0

Client Name: mfwd (comp-id: 0x348)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0

Client Name: PBR_EA (comp-id: 0x1277)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0

Client Name: bfd_agent (comp-id: 0x859)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
```

```
# of ECD Pathlist: 0

Client Name: IPV4_ABF (comp-id: 0x1e01)
------------
Protocol           : ipv4
# of Registrations : 0
# of Pending notifs: 0
Client last pulsed : Never
ECD version: 1
# of ECD Pathlist: 0
```

Related Commands

Command	Description
show cef, on page 162	Displays information about packets forwarded by Cisco Express Forwarding (CEF).

show cef ipv4 adjacency

To display Cisco Express Forwarding (CEF) IPv4 adjacency status and configuration information, use the **show cef ipv4 adjacency** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 adjacency** [*interface-type interface-path-id*] [**location** *node-id*] [**detail**] [**discard**] [**glean**] [**null**] [**punt**] [**remote**] [**protected**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays the detailed adjacency information.
discard	(Optional) Filters out and displays only the discarded adjacency information.
glean	(Optional) Filters out and displays only the glean adjacency information.
null	(Optional) Filters out and displays only the adjacency information.
punt	(Optional) Filters out and displays only the punt adjacency information.
remote	(Optional) Filters out and displays only the remote adjacency information.
protected	(Optional) Filters out and displays only the IP-Fast Reroute (FRR) protected adjacency information.

Command Default

No default behavior or values

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef ipv4 adjacency** command displays the CEF adjacency table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from **show cef ipv4 adjacency** command :

```
Router# show cef ipv4 adjacency

Display protocol is ipv4
Interface    Address                                          Type    Refcount

Hu0/6/0/16                                                    special 2
             Interface: Hu0/6/0/16 Type:  glean
             Interface Type: 0x0, Base Flags: 0x220 (0x8ceb3f98)
             Nhinfo PT: 0x8ceb3f98, Idb PT: 0x8cb35a20,
             If Handle: 0x30001e0 no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec  7 11:20:35.145


Hu0/6/0/16  Prefix: 10.0.22.2/32                             local   9
            Adjacency: PT:0x8d5752b8 10.0.22.2/32
            Interface: Hu0/6/0/16
            NHID: 0x0
            MAC: e6.07.2b.8d.33.f0.e6.48.5c.10.b3.a0.08.00
            Interface Type: 0x0, Base Flags: 0x1 (0x8d001fa0)
            Nhinfo PT: 0x8d001fa0, Idb PT: 0x8cb35a20,
            If Handle: 0x30001e0 no dependent adj
            Ancestor If Handle: 0x0
Update time Dec  7 11:20:45.022


Hu0/6/0/18                                                    special 2
             Interface: Hu0/6/0/18 Type:  glean
             Interface Type: 0x0, Base Flags: 0x220 (0x8ceb44c0)
             Nhinfo PT: 0x8ceb44c0, Idb PT: 0x8cb35920,
             If Handle: 0x30001f0 no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec  7 11:20:33.449


Hu0/6/0/18   Prefix: 10.0.62.2/32                             local   10
             Adjacency: PT:0x8d5794a0 10.0.62.2/32
             Interface: Hu0/6/0/18
             NHID: 0x0
             MAC: e6.07.2b.8d.34.48.e6.48.5c.10.b3.a8.08.00
             Interface Type: 0x0, Base Flags: 0x1 (0x8d002aa0)
             Nhinfo PT: 0x8d002aa0, Idb PT: 0x8cb35920
             If Handle: 0x30001f0 no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec  7 11:20:45.019
```

This table describes the significant fields shown in the display.

Table 9: show cef ipv4 adjacency Command Field Descriptions

Field	Description
Interface	Interface associated with the prefix.
Address	Prefix address information.
Type	Type of adjacency, can be either local or remote.
Refcount	Number of times the adjacency is referenced by other routers.

show cef ipv4 adjacency hardware

To display Cisco Express Forwarding (CEF) IPv4 adjacency hardware status and configuration information, use the **show cef ipv4 adjacency hardware** command in XR EXEC mode.

show cef[**vrf** *vrf-name*] **ipv4 adjacency hardware** {**egress**} [**detail** | **discard** | **drop** | **glean** | **location** *node-id* | **null** | **punt** | **protected** | **remote**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
egress	Displays information from the egress packets.
detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
protected	(Optional) Filters out and displays only the IP-Fast Reroute (FRR) protected adjacency information.
remote	(Optional) Displays the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output shows the load information flag from the **show cef ipv4 adjacency hardware** command for the **egress** keyword:

```
Router# show cef ipv4 adjacency hardware egress detail location 0/RP0/CPU0
Tue Apr 28 04:15:15.408 UTC
Display protocol is ipv4
Interface    Address                                         Type    Refcount

BE3                                                          special 2
             Interface: BE3 Type:  glean
             Interface Type: 0x1c, Base Flags: 0x10001100 (0x8deeece0)
             Nhinfo PT: 0x8deeece0, Idb PT: 0x8db2a1c0, If Handle: 0xf00001c
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 03:49:04.881


BE3           Prefix: 9.1.48.4/32                            local   5
             Adjacency: PT:0x8e68d1b8 9.1.48.4/32
             Interface: BE3
             NHID: 0x0
             MAC: 78.70.32.67.6d.03.b0.65.62.36.20.03.08.00
             Interface Type: 0x1c, Base Flags: 0x10000001 (0x8fa2a0b0)
             Nhinfo PT: 0x8fa2a0b0, Idb PT: 0x8db2a1c0, If Handle: 0xf00001c
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 03:49:05.238


BE4                                                          special 2
             Interface: BE4 Type:  glean
             Interface Type: 0x1c, Base Flags: 0x10001100 (0x8deeed68)
             Nhinfo PT: 0x8deeed68, Idb PT: 0x8db2a250, If Handle: 0xf000024
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 03:49:04.884


BE4           Prefix: 9.1.58.5/32                            local   7
             Adjacency: PT:0x8e68d548 9.1.58.5/32
             Interface: BE4
             NHID: 0x0
             MAC: 78.46.8e.f2.f9.03.b0.65.62.36.20.02.08.00
             Interface Type: 0x1c, Base Flags: 0x10000001 (0x8fa2a260)
             Nhinfo PT: 0x8fa2a260, Idb PT: 0x8db2a250, If Handle: 0xf000024
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 04:05:26.678


BE28                                                         special 2
             Interface: BE28 Type:  glean
             Interface Type: 0x1c, Base Flags: 0x10001100 (0x8deeedf0)
             Nhinfo PT: 0x8deeedf0, Idb PT: 0x8db2a2e0, If Handle: 0xf00002c
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 03:49:04.884


BE28          Prefix: 9.9.28.2/32                            local   7
             Adjacency: PT:0x8e68d2e8 9.9.28.2/32
             Interface: BE28
             NHID: 0x0
             MAC: 78.70.d8.38.0d.03.b0.65.62.36.20.01.08.00
             Interface Type: 0x1c, Base Flags: 0x10000001 (0x8fa2a140)
             Nhinfo PT: 0x8fa2a140, Idb PT: 0x8db2a2e0, If Handle: 0xf00002c
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 04:04:30.218


BE2801                                                       special 2
             Interface: BE2801 Type:  glean
             Interface Type: 0x1c, Base Flags: 0x10001100 (0x8deeee78)
             Nhinfo PT: 0x8deeee78, Idb PT: 0x8db2a370, If Handle: 0xf000034
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 03:49:04.884


BE2801        Prefix: 10.28.1.2/32                           local   7
             Adjacency: PT:0x8e68d418 10.28.1.2/32
             Interface: BE2801
             NHID: 0x0
             MAC: 78.70.d8.38.0d.02.b0.65.62.36.20.00.08.00
             Interface Type: 0x1c, Base Flags: 0x10000001 (0x8fa2a1d0)
             Nhinfo PT: 0x8fa2a1d0, Idb PT: 0x8db2a370, If Handle: 0xf000034
no dependent adj
             Ancestor If Handle: 0x0
 Update time Apr 28 04:04:30.218
```

show cef ipv4

To display the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4** [*prefix* [*mask*] | *interface-type interface-instance*] [**detail**] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
prefix	(Optional) Longest matching CEF entry for the specified IPv4 destination prefix.
mask	(Optional) Exact CEF entry for the specified IPv4 prefix and mask.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-instance	Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface MgmtEth0/RP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays full CEF entry information.
location *node-id*	(Optional) Displays the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If the location is not specified, the command defaults to the active RP node.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF table on the node in which the command is issued. Otherwise, the command is effective on the node specified by the **location** *node-id* keyword and argument.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4** command:

```
Router# show cef ipv4
Prefix              Next Hop            Interface
------------------- ------------------- ------------------
0.0.0.0/0           drop                default handler
0.0.0.0/32          broadcast
1.75.55.1/32        1.76.0.1/32         <recursive>
1.76.0.0/16         attached            MgmtEth0/RP0/CPU0/0
1.76.0.0/32         broadcast           MgmtEth0/RP0/CPU0/0
1.76.0.1/32         1.76.0.1/32         MgmtEth0/RP0/CPU0/0
1.76.0.2/32         1.76.0.2/32         MgmtEth0/RP0/CPU0/0
1.76.0.3/32         1.76.0.3/32         MgmtEth0/RP0/CPU0/0
1.76.11.2/32        1.76.11.2/32        MgmtEth0/RP0/CPU0/0


Router# show cef ipv4
Prefix              Next Hop            Interface
------------------- ------------------- ------------------
0.0.0.0/0           drop                default handler
0.0.0.0/32          broadcast
1.75.55.1/32        1.76.0.1/32         <recursive>
1.76.0.0/16         attached            MgmtEth0/RP0/CPU0/0
1.76.0.0/32         broadcast           MgmtEth0/RP0/CPU0/0
1.76.0.1/32         1.76.0.1/32         MgmtEth0/RP0/CPU0/0
1.76.0.2/32         1.76.0.2/32         MgmtEth0/RP0/CPU0/0
1.76.0.3/32         1.76.0.3/32         MgmtEth0/RP0/CPU0/0
1.76.11.2/32        1.76.11.2/32        MgmtEth0/RP0/CPU0/0
```

This table describes the significant fields shown in the display.

Table 10: show cef ipv4 Command Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

show cef ipv4 drops

To display IPv4 Cisco Express Forwarding (CEF) table packet drop counters, use the **show cef ipv4 drops** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 drops** [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
location *node-id*	(Optional) Displays IPv4 CEF table packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A packet might be dropped from the IPv4 CEF table because of unresolved CEF entries, unsupported features, absence of route information, absence of adjacency information, or an IP checksum error.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays IPv4 CEF packet drop counters for all nodes.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 drops** for location command:

```
Router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :               0
  No route drops       packets :               0
  No Adjacency drops   packets :               0
  Checksum error drops packets :               0
  RPF drops            packets :               0
  RPF suppressed drops packets :               0
  RP destined drops    packets :               0
  Discard drops        packets :               0
  GRE lookup drops     packets :               0
  GRE processing drops packets :               0
  LISP punt drops      packets :               0
  LISP encap err drops packets :              0
  LISP decap err drops packets :              0

Node: 0/RP1/CPU0
  Unresolved drops     packets :              0
  Unsupported drops    packets :              0
  Null0 drops          packets :              0
  No route drops       packets :              0
  No Adjacency drops   packets :              0
  Checksum error drops packets :              0
  RPF drops            packets :              0
  RPF suppressed drops packets :              0
  RP destined drops    packets :              0
  Discard drops        packets :              0
  GRE lookup drops     packets :              0
  GRE processing drops packets :              0
  LISP punt drops      packets :              0
  LISP encap err drops packets :              0
  LISP decap err drops packets :              0
```

Table 11: show cef ipv4 drop Command Field Descriptions

Field	Description
Unresolved drops	Drops due to unresolved routes.
Unsupported drops	Drops due to an unsupported feature.
Null0 drops	Drops to the Null0 interface.
No route drops	Number of packets dropped because there were no routes to the destination.
No Adjacency drops	Number of packets dropped because there were no adjacencies established.
Checksum error drops	Drops due to IPv4 checksum error.
RPF drops	Drops due to IPv4 unicast RPF[1].
RPF suppressed drops	Drops suppressed due to IPv4 unicast RPF.
RP destined drops	Drops destined for the router.
Discard drops	Drops those were discarded.
GRE lookup drops	GRE packets dropped during GRE Lookup.
GRE processing drops	GRE packets dropped during GRE Processing.
LISP punt drops	LISP packets dropped during software processing of the packets.
LISP encap err drops	LISP encap packets dropped due to errors.
LISP decap err drops	LISP Decap packets dropped due to errors.

[1] RPF = Reverse Path Forwarding

show cef ipv4 exact-route

To display an IPv4 Cisco Express Forwarding (CEF) exact route, use the **show cef ipv4 exact-route** command in XR EXEC mode.

show cef [**vrf** *vrf-name*]**ipv4 exact-route** {*source-address destination-address*} [**protocol***protocol-name*] [**source-port***source-port*] [**destination-port***destination-port*] [*type interface-path-id*] [*policy-class-value*] [**detail | location** *node-id*] { **ingress-interface** *ingress-interface* | **user-data** *user-data* **ingress-interface** *ingress-interface* [**brief** | **detail** | **hardware** | **internal** | **location** | **policy-class** | **protocol**] }

Syntax Description

vrf	(Optional) Sets VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
source-address	The IPv4 source address in x.x.x.x format.
destination-address	The IPv4 destination address in x.x.x.x format.
protocol *protocol name*	(Optional) Sets the specified protocol for the route.
source-port *source-port*	(Optional) Sets the TCP and UDP source port. The range is from 0 to 65535.
destination-port *destination-port*	(Optional) Sets the TCP and UDP destination port. The range is from 0 to 65535.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Provides full CEF entry information.
location *node-id*	(Optional) Provides the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
ingress-interface	(Optional) Specifies the ingress interface information.
user-data *user-data*	(Optional) Specifies the additional user chosen data bytes used in multi-path computation. In *user-data*, you can enter 1-4 bytes in hexadecimal.
ingress-interface *ingress-interface*	Specifies the ingress interface information.
brief	(Optional) Displays brief information of CEF table.

detail	(Optional) Displays full information of CEF table.
hardware	(Optional) Displays information from hardware.
location	(Optional) Provides the forwarding information for the designated node. The node-id argument is entered in the *rack/slot/module* notation.
policy-class	(Optional) Class for policy-based tunnel selection.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.5	The keyword **user-data** was introduced.
Release 24.2.11	The keyword **user-data** was introduced.
Release 7.0.12	This command was introduced.

Usage Guidelines

For TCP and UDP protocols, configure the source-port and destination-port mandatorily. For other protocols, configure the source-port and destination-port as zero. Otherwise, the output of the **show cef ipv4 exact-route** command is not correct.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4 exact-route** command:

```
Router# show cef ipv4 exact-route 192.0.2.1 198.51.100.1 protocol TCP source-port 25000
destination-port 30000 ingress-interface HundredGigE 0/0/0/24
Wed Apr 15 02:15:16.102 UTC
5.5.5.5/32, version 18, labeled SR, internal 0x1000001 0x8110 (ptr 0x94730608) [1], 0x0
(0x94710b18), 0xa28 (0x9849c0a8)
 Updated Apr 14 19:08:57.655 local adjacency 30.0.0.2
 Prefix Len 32, traffic index 0, precedence n/a, priority 1, encap-id 0x1000800000001
   via Bundle-Ether3
   via 30.0.0.2/32, Bundle-Ether3, 7 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 1 NHID 0x0 [0x97b2d338 0x0]
    next hop 30.0.0.2/32
     local adjacency
      local label 21555 labels imposed {21555}
```

The following is a sample output of the **show cef ipv4 exact-route** command with **user-data** keyword:

```
Router# show cef ipv4 exact-route 100.0.0.10 60.1.0.1 protocol 253 source-port 0
destination-port 0 user-data 0x4 ingress-interface HundredGigE0/0/0/2 location 0/0/cpu0

Mon Aug 14 07:56:18.145 UTC
```

```
Unsupported protocol value 253
48.0.0.0/4, version 1377, internal 0x1000001 0x20 (ptr 0x8b470510) [1], 0x400 (0x8e0d45e8),
 0x0 (0x0)
 Updated Aug 14 07:50:20.022
 local adjacency to HundredGigE0/0/0/26.29

 Prefix Len 4, traffic index 0, precedence n/a, priority 2
   via HundredGigE0/0/0/26.29
   via 34.0.9.2/32, HundredGigE0/0/0/26.29, 5 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 1 NHID 0x0 [0x8c60c480 0x0]
    next hop 34.0.9.2/32
    local adjacency
```

This table describes the significant fields shown in the display.

Table 12: show cef ipv4 exact-route Command Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table .
Next Hop	Next hop of the prefix
Interface	Interface associated with the prefix

show cef ipv4 exceptions

To display IPv4 Cisco Express Forwarding (CEF) exception packet counters, use the **show cef ipv4 exceptions** command in .

show **cef** [**vrf** *vrf-name*] **ipv4** **exceptions** [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
location *node-id*	(Optional) Displays CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

CEF exception packets are those packets that have been sent from the hardware to the software because they require additional handling. The types of IPv4 CEF exception packets are displayed in the command’s output and are defined.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays IPv4 CEF exception packet counters on all nodes.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 exceptions** command:

```
Router# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :               0
  Unsupported packets :               0
  Redirect    packets :               0
  Receive     packets :               0
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0
Node: 0/RP1/CPU0
  Slow encap  packets :               3
  Unsupported packets :               0
  Redirect    packets :               0
```

```
Receive     packets :          12787
Broadcast   packets :          74814
IP options  packets :              0
TTL expired packets :              0
Fragmented  packets :              0
```

This table describes the significant fields shown in the display.

Table 13: show cef ipv4 exceptions Command Field Descriptions

Field	Description
Slow encap	Number of packets requiring special processing during encapsulation.
Redirect	Number of ICMP[2] redirect messages sent.
Receive	Number of packets destined to the router.
Broadcast	Number of broadcasts received.
IP options	Number of IP option packets.
TTL expired	Number of packets with expired TTLs[3].
Fragmented	Number of packets that have been fragmented.

[2] ICMP = internet control message protocol
[3] TTL = time to live

show cef ipv4 hardware

To display Cisco Express Forwarding (CEF) IPv4 hardware status and configuration information, use the **show cef ipv4 hardware** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 hardware** {**egress** | [**detail** | **location** *node-id*]}

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
egress	Displays information from the egress packets.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4 hardware** command:

```
Router# show cef ipv4 hardware egress detail location 0/RP0/CPU0

Wed Apr 22 09:06:45.028 UTC
0.0.0.0/0, version 0, proxy default, default route handler, drop adjacency, internal 0x1001011
 0x0 (ptr 0x919f10b8) [1], 0x0 (0x919bf0a8), 0x0 (0x0)
 Updated Apr 22 09:03:29.837
 Prefix Len 0, traffic index 0, precedence n/a, priority 15
  gateway array (0x918320a8) reference count 1, flags 0x200, source default (12), 0 backups

                [2 type 3 flags 0xa401 (0x918e50a8) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0x919bf0a8, sh-ldi=0x918e50a8]
  gateway array update type-time 1 Apr 22 09:03:29.838
 LDI Update time Apr 22 09:03:29.881
 LW-LDI-TS Apr 22 09:03:29.881
```

```
   via 0.0.0.0/32, 3 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0x90e9d810 0x0]
    next hop 0.0.0.0/32
     drop adjacency

 Show-data Print at RPLC


 LEAF - HAL pd context :
 sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    trans_id: 29
    PI_ctx: 0x30919f10b8
    eng_ctx: 0x30919f1158
    revision: 29
    hal_leaf_type: IPV4
    created_in_ofa: 1
    NHGROUP_key:  {ID: 24-14-00-10-01-00-00-00}
    leaf npd data:

[illegible]


FIB_HAL_OBJECT_NRLWLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 28
  engctx: 0x30919bf0e8

FIB_HAL_OBJECT_SHLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 27
  engctx: 0x30918e5178
  nhgroup
    key: 24140010 01000000
    num paths: 1
    oor_state: 0
    is_protected[0]: 0
    next_obj[0] type: 6
    next_obj[0] exceptionnh key: type,4, intf,0, proto,0
  nhgroup npd data:
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
c_nextobj_ip6llnhtnh=NS,0:rdesc_nextobj_nhgrouptnh=NS

HW Walk:
LEAF:
    trans_id: 29
    PI_ctx: 0x30919f10b8
    eng_ctx: 0x30919f1158
    revision: 29
    hal_leaf_type: IPV4
    created_in_ofa: 1
    NHGROUP_key:  {ID: 24-14-00-10-01-00-00-00}
    leaf npd data:

[illegible]
```

```
    Load distribution: 0 (refcount 2)

    Hash  OK  Interface                 Address
    0     Y   recursive                 drop
0.0.0.0/32, version 0, broadcast
  Updated Apr 22 09:03:29.912
  Prefix Len 32

 Show-data Print at RPLC


 LEAF - HAL pd context :
 sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    trans_id: 35
    PI_ctx: 0x30919f1298
    eng_ctx: 0x30919f1338
    revision: 35
    hal_leaf_type: IPV4
    created_in_ofa: 1
    ExceptionNH_key: {type: 2, proto: 0, l3addr: 0.0.0.0}
    leaf npd data:

[illegible]


FIB_HAL_OBJECT_NRLWLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 34
  engctx: 0x30919c0438

FIB_HAL_OBJECT_SHLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 33
  engctx: 0x30918e65f8

HW Walk:
LEAF:
    trans_id: 35
    PI_ctx: 0x30919f1298
    eng_ctx: 0x30919f1338
    revision: 35
    hal_leaf_type: IPV4
    created_in_ofa: 1
    ExceptionNH_key: {type: 2, proto: 0, l3addr: 0.0.0.0}
    leaf npd data:

[illegible]
224.0.0.0/4, version 0, external adjacency, internal 0x1040001 0x0 (ptr 0x919f1478) [1],
0x0 (0x919c1748), 0x0 (0x0)
 Updated Apr 22 09:03:29.916
 Prefix Len 4, traffic index 0, precedence n/a, priority 15
  gateway array (0x91832448) reference count 1, flags 0x0, source special (1), 0 backups
                [2 type 3 flags 0x8401 (0x918e79a8) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0x919c1748, sh-ldi=0x918e79a8]
  gateway array update type-time 1 Apr 22 09:03:29.916
 LDI Update time Apr 22 09:03:29.916
 LW-LDI-TS Apr 22 09:03:29.916
   via 0.0.0.0/32, 3 dependencies, weight 0, class 0 [flags 0x0]
```

```
    path-idx 0 NHID 0x0 [0x90e9e468 0x0]
    next hop 0.0.0.0/32
     external adjacency

 Show-data Print at RPLC


 LEAF - HAL pd context :
 sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    trans_id: 41
    PI_ctx: 0x30919f1478
    eng_ctx: 0x30919f1518
    revision: 41
    hal_leaf_type: IPV4
    created_in_ofa: 1
    NHGROUP_key:  {ID: 24-14-00-10-02-00-00-00}
    leaf npd data:

[illegible]


FIB_HAL_OBJECT_NRLWLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 40
  engctx: 0x30919c1788

FIB_HAL_OBJECT_SHLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 39
  engctx: 0x30918e7a78
  nhgroup
    key: 24140010 02000000
    num paths: 1
    oor_state: 0
    is_protected[0]: 0
    next_obj[0] type: 6
    next_obj[0] exceptionnh key: type,1, intf,0, proto,0
  nhgroup npd data:
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
nextobj_ip6llnhtnh=NS,0:rdesc_nextobj_nhgrouptnh=NS

HW Walk:
LEAF:
    trans_id: 41
    PI_ctx: 0x30919f1478
    eng_ctx: 0x30919f1518
    revision: 41
    hal_leaf_type: IPV4
    created_in_ofa: 1
    NHGROUP_key:  {ID: 24-14-00-10-02-00-00-00}
    leaf npd data:

[illegible]
```

```
    Load distribution: 0 (refcount 2)

    Hash  OK  Interface                 Address
    0     Y   recursive                 external
224.0.0.0/24, version 0, receive
  Updated Apr 22 09:03:29.912
  Prefix Len 24
  internal 0x1004001 (ptr 0x919f1388) [1], 0x0 (0x919c0da0), 0x0 (0x0)
, receive adjacency, internal 0x1004001 0x0 (ptr 0x919f1388) [1], 0x0 (0x919c0da0), 0x0
(0x0)
 Updated Apr 22 09:03:29.912
 Prefix Len 24, traffic index 0, precedence n/a, priority 15
  gateway array (0x91832360) reference count 1, flags 0x0, source special (1), 0 backups
                [2 type 3 flags 0x8401 (0x918e6f68) ext 0x0 (0x0)]
  LW-LDI[type=3, refc=1, ptr=0x919c0da0, sh-ldi=0x918e6f68]
  gateway array update type-time 1 Apr 22 09:03:29.911
 LDI Update time Apr 22 09:03:29.911
 LW-LDI-TS Apr 22 09:03:29.911
   via 0.0.0.0/32, 11 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0x90e9dd00 0x0]
    next hop 0.0.0.0/32
     receive adjacency

 Show-data Print at RPLC


 LEAF - HAL pd context :
 sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    trans_id: 38
    PI_ctx: 0x30919f1388
    eng_ctx: 0x30919f1428
    revision: 38
    hal_leaf_type: IPV4
    created_in_ofa: 1
    ExceptionNH_key: {type: 1, proto: 0, l3addr: 0.0.0.0}
    leaf npd data:

[illegible]


FIB_HAL_OBJECT_NRLWLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 37
  engctx: 0x30919c0de0

FIB_HAL_OBJECT_SHLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 36
  engctx: 0x30918e7038

HW Walk:
LEAF:
    trans_id: 38
    PI_ctx: 0x30919f1388
    eng_ctx: 0x30919f1428
    revision: 38
    hal_leaf_type: IPV4
    created_in_ofa: 1
    ExceptionNH_key: {type: 1, proto: 0, l3addr: 0.0.0.0}
    leaf npd data:

[illegible]


    Load distribution: 0 (refcount 2)

    Hash  OK  Interface                 Address
    0     Y   recursive                 receive
255.255.255.255/32, version 0, broadcast
  Updated Apr 22 09:03:29.905
  Prefix Len 32

 Show-data Print at RPLC


 LEAF - HAL pd context :
 sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    trans_id: 32
    PI_ctx: 0x30919f11a8
    eng_ctx: 0x30919f1248
    revision: 32
    hal_leaf_type: IPV4
    created_in_ofa: 1
    ExceptionNH_key: {type: 2, proto: 0, l3addr: 0.0.0.0}
    leaf npd data:

[illegible]


FIB_HAL_OBJECT_NRLWLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 31
  engctx: 0x30919bfa90

FIB_HAL_OBJECT_SHLDI:
  hal_proto: 12
  trans_id: 0
  prev_trans_id: 30
  engctx: 0x30918e5bb8

HW Walk:
LEAF:
    trans_id: 32
    PI_ctx: 0x30919f11a8
    eng_ctx: 0x30919f1248
    revision: 32
    hal_leaf_type: IPV4
    created_in_ofa: 1
    ExceptionNH_key: {type: 2, proto: 0, l3addr: 0.0.0.0}
    leaf npd data:

[illegible]
```

show cef ipv4 interface

To display IPv4 Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef ipv4 interface** command in XR EXEC mode.

show cef[**vrf** *vrf-name*] **ipv4 interface** *type interface-path-id* [**detail**] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	Interface type. For more information, use the question mark (?) online help function.
in terface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface HundredGigE 0/RP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
location *node-id*	(Optional) Displays IPv4 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef ipv4 interface rpf-statistics** command displays the CEF-related information for the interface on the route processor.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 interface** command:

```
Router# show cef ipv4 interface  HundredGigE 0/0/0/24
HundredGigE0/0/0/0 is up if_handle 0x0f000138 if_type IFT_HUNDREDGE(0x49)
     idb info 0x9093e730 flags 0x8001 ext 0x942c8da8 flags 0x50
     Vrf Local Info (0x95106328)
  Interface last modified Jan 13, 2020 06:08:29, create
  Reference count 1       Next-Hop Count 2
  Forwarding is enabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 1500, TableId 0xe0000000(0x90d43400)
  Protocol Reference count 2
  Primary IPV4 local address 100.0.0.6/32
```

This table describes the significant fields shown in the display.

Table 14: show cef ipv4 interface Command Field Descriptions

Field	Description
HundredGigE0/0/0/24 is down	Status of the interface.
if_handle	Internal interface handle.
Forwarding is enabled	Indicates that Cisco Express Forwarding (CEF) is enabled.
ICMP redirects are always sent or never sent	Indicates whether ICMP[4] redirect messages should be sent. By default, ICMP redirect messages are always sent.
IP MTU	Value of the IPv4 MTU[5] size set on the interface.
Reference count	Internal reference counter.

[4] ICMP = internet control message protocol

[5] MTU = maximum transmission unit

show cef ipv4 non-recursive

To display the IPv4 nonrecursive prefix entries in the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 non-recursive** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 non-recursive** [**detail**] [**hardware** {**egress** | **ingress**}] [*interface-type interface-instance*] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
detail	(Optional) Displays detailed information about nonrecursive prefix entries in the IPv4 CEF table.
hardware	(Optional) Displays detailed information about hardware.
egress	(Optional) Displays egress NPU.
ingress	(Optional) Displays ingress NPU.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-instance	(Optional) Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface MgmtEth0/RP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays the IPv4 nonrecursive prefix entries in the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the IPv4 CEF nonrecursive routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 non-recursive** command:

```
Router# show cef ipv4 non-recursive

Prefix              Next Hop            Interface
0.0.0.0/0           1012.8.0.1
0.0.0.0/32          broadcast
10.8.0.0/16         attached            MgmtEth0/0/CPU0/0
10.8.0.0/32         broadcast           MgmtEth0/0/CPU0/0
10.8.0.1/32         12.8.0.1            MgmtEth0/0/CPU0/0
10.8.0.2/32         12.8.0.2            MgmtEth0/0/CPU0/0
10.8.0.3/32         12.8.0.3            MgmtEth0/0/CPU0/0
10.8.16.10/32       12.8.16.10          MgmtEth0/0/CPU0/0
10.8.16.30/32       12.8.16.30          MgmtEth0/0/CPU0/0
10.8.16.40/32       12.8.16.40          MgmtEth0/0/CPU0/0
10.8.28.8/32        12.8.28.8           MgmtEth0/0/CPU0/0
10.8.28.101/32      12.8.28.101         MgmtEth0/0/CPU0/0
10.8.28.103/32      12.8.28.103         MgmtEth0/0/CPU0/0
10.8.28.104/32      12.8.28.104         MgmtEth0/0/CPU0/0
10.8.28.106/32      receive             MgmtEth0/0/CPU0/0
10.8.29.113/32      12.8.29.113         MgmtEth0/0/CPU0/0
10.8.29.118/32      12.8.29.118         MgmtEth0/0/CPU0/0
10.8.29.140/32      12.8.29.140         MgmtEth0/0/CPU0/0
10.8.33.101/32      12.8.33.101         MgmtEth0/0/CPU0/0
10.8.33.103/32      12.8.33.103         MgmtEth0/0/CPU0/0
10.8.33.105/32      12.8.33.105         MgmtEth0/0/CPU0/0
10.8.33.110/32      12.8.33.110         MgmtEth0/0/CPU0/0
10.8.57.1/32        12.8.57.1           MgmtEth0/0/CPU0/0
10.8.255.255/32     broadcast           MgmtEth0/0/CPU0/0
10.29.31.2/32       12.29.31.2          MgmtEth0/0/CPU0/0
10.255.0.0/16            attached        MgmtEth0/0/CPU0/0
10.255.254.254/32   10223.255.254.254     MgmtEth0/0/CPU0/0
10.0.0.0/4            0.0.0.0
10.0.0.0/24         receive
255.255.255.255/32   broadcast
```

This table describes the significant fields shown in the display.

Table 15: show cef ipv4 non-recursive Command Field Descriptions

Field	Description
Prefix	Nonrecursive prefixes detected on the node.

Field	Description
Next Hop	Routing next hop.
Interface	Interface associated with the nonrecursive prefix.

show cef ipv4 resource

To display the IPv4 nonrecursive prefix entries in the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 resource** command in XR EXEC mode.

show **cef** **ipv4** **resource** [**detail**] [**hardware** { **egress** | **ingress** }] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed information resources listed in the IPv4 CEF table.
location *node-id*	(Optional) Displays the IPv4 resource entries in the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the IPv4 CEF nonrecursive routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 resource** command:

```
Router# show cef ipv4 resource detail

CEF resource availability summary state: GREEN
CEF will work normally
  ipv4 shared memory resource:
        CurrMode GREEN, CurrAvail 7167668222 bytes, MaxAvail 7242276863 bytes
  ipv6 shared memory resource:
        CurrMode GREEN, CurrAvail 7167668222 bytes, MaxAvail 7242276863 bytes
  mpls shared memory resource:
        CurrMode GREEN, CurrAvail 7167668222 bytes, MaxAvail 7242276863 bytes
  common shared memory resource:
        CurrMode GREEN, CurrAvail 7167668222 bytes, MaxAvail 7242276863 bytes
  DATA_TYPE_TABLE_SET hardware resource: GREEN
  DATA_TYPE_TABLE hardware resource: GREEN
  DATA_TYPE_IDB hardware resource: GREEN
  DATA_TYPE_IDB_EXT hardware resource: GREEN
  DATA_TYPE_LEAF hardware resource: GREEN
  DATA_TYPE_LOADINFO hardware resource: GREEN
  DATA_TYPE_PATH_LIST hardware resource: GREEN
  DATA_TYPE_NHINFO hardware resource: GREEN
```

```
DATA_TYPE_LABEL_INFO hardware resource: GREEN
DATA_TYPE_FRR_NHINFO hardware resource: GREEN
DATA_TYPE_ECD hardware resource: GREEN
DATA_TYPE_RECURSIVE_NH hardware resource: GREEN
DATA_TYPE_TUNNEL_ENDPOINT hardware resource: GREEN
DATA_TYPE_LOCAL_TUNNEL_INTF hardware resource: GREEN
DATA_TYPE_ECD_TRACKER hardware resource: GREEN
DATA_TYPE_ATTRIBUTE hardware resource: GREEN
DATA_TYPE_LSPA hardware resource: GREEN
DATA_TYPE_LDI_LW hardware resource: GREEN
DATA_TYPE_LDSH_ARRAY hardware resource: GREEN
DATA_TYPE_TE_TUN_INFO hardware resource: GREEN
DATA_TYPE_DUMMY hardware resource: GREEN
DATA_TYPE_IDB_VRF_LCL_CEF hardware resource: GREEN
DATA_TYPE_PROTO_GBL hardware resource: GREEN
DATA_TYPE_MOL hardware resource: GREEN
DATA_TYPE_MPI hardware resource: GREEN
DATA_TYPE_SUBS_INFO hardware resource: GREEN
DATA_TYPE_LISP_IPENCAP hardware resource: GREEN
DATA_TYPE_LSM_ID hardware resource: GREEN
DATA_TYPE_INTF_LIST hardware resource: GREEN
DATA_TYPE_TUNNEL_ENCAP_STR hardware resource: GREEN
DATA_TYPE_LABEL_RPF hardware resource: GREEN
DATA_TYPE_L2_SUBS_INFO hardware resource: GREEN
DATA_TYPE_LISP_IID_MAPPING hardware resource: GREEN
DATA_TYPE_LISP_RLOC_TBL hardware resource: GREEN
DATA_TYPE_NHID hardware resource: GREEN
DATA_TYPE_LOOKUP hardware resource: GREEN
DATA_TYPE_PREFIX_FILTER hardware resource: GREEN
DATA_TYPE_PREFIX_FILTER_TBL hardware resource: GREEN
DATA_TYPE_LLC_TBL hardware resource: GREEN
DATA_TYPE_LLC hardware resource: GREEN
DATA_TYPE_TI_PL_TBL hardware resource: GREEN
DATA_TYPE_RETRY_TBL hardware resource: GREEN
DATA_TYPE_RETRY hardware resource: GREEN
DATA_TYPE_OBJECT_QUEUE_HEAD hardware resource: GREEN
DATA_TYPE_OBJECT_MARKER hardware resource: GREEN
DATA_TYPE_PL_TRKR_ENTRY hardware resource: GREEN
DATA_TYPE_PL_TRKR_SHARE_NH hardware resource: GREEN
DATA_TYPE_NH_TRKR_SHARE_NH hardware resource: GREEN
DATA_TYPE_LEAF_TRKR_SHARE_NH hardware resource: GREEN
DATA_TYPE_FRR_NH_TRKR_SHARE_NH hardware resource: GREEN
DATA_TYPE_NH_REPL hardware resource: GREEN
DATA_TYPE_LEAF_EXT hardware resource: GREEN
DATA_TYPE_QUEUE_EXT hardware resource: GREEN
DATA_TYPE_COFO_TBL hardware resource: GREEN
DATA_TYPE_COFO_TBL_ENTRY hardware resource: GREEN
DATA_TYPE_COFO_IDB_TBL hardware resource: GREEN
DATA_TYPE_COFO_IDB_ENTRY hardware resource: GREEN
DATA_TYPE_DELETED_OBJECT_TBL hardware resource: GREEN
DATA_TYPE_DELETED_OBJECT hardware resource: GREEN
DATA_TYPE_SR6_GBL hardware resource: GREEN
DATA_TYPE_SR6A hardware resource: GREEN
DATA_TYPE_SR6I hardware resource: GREEN
DATA_TYPE_TEP hardware resource: GREEN
DATA_TYPE_LTEP hardware resource: GREEN
DATA_TYPE_TES hardware resource: GREEN
DATA_TYPE_ENCAP hardware resource: GREEN
DATA_TYPE_ENCAP_ARRAY hardware resource: GREEN
DATA_TYPE_ENCAP_IDA hardware resource: GREEN
DATA_TYPE_ENCAP_ID_TBL hardware resource: GREEN
DATA_TYPE_ENCAP_ID hardware resource: GREEN
```

show cef ipv4 summary

To display a summary of the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 summary** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 summary** [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
location *node-id*	(Optional) Displays a summary of the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays a summary of the IPv4 CEF table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv4 summary** command:

```
Router# show cef ipv4 summary
Router ID is
10
0
.0.0.0

IP CEF with switching (Table Version 0)

  Load balancing: L3
  Tableid 0xe0000000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
  Vrfname default, Refcount 367
  193 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 13896 bytes
  204 load sharing elements, 51904 bytes, 154 references
  17 shared load sharing elements, 5536 bytes
  187 exclusive load sharing elements, 46368 bytes
  0 CEF route update drops, 175 revisions of existing leaves
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  16 prefixes with label imposition, 51 prefixes with label information
Adjacency Table has 44 adjacencies
  1 incomplete adjacency
```

This table describes the significant fields shown in the display.

Table 16: show cef ipv4 summary Command Field Descriptions

Field	Description
Load balancing	Current load-balancing mode. The default value is L3.
Table Version	Version of the CEF table.
tableid	Table identification number.
vrfid	VPN routing and forwarding (VRF) identification (vrfid) number.
vrfname	VRF name.
vrid	Virtual router identification (vrid) number.
flags	Option value for the table
routes	Total number of routes.
reresolve	Total number of routes being reresolved.
unresolved (*x* old, *x* new)	Number of routes not yet resolved.
load sharing elements	Total number of internal load-sharing data structures.
bytes	Total memory used by internal load sharing data structures.
references	Total reference count of all internal load sharing data structures.
CEF resets	Number of CEF table resets.
revisions of existing leaves	Number of updates to existing prefixes.
Exponential (currently *x*s, peak *x*s)	Currently not used.
prefixes modified in place	Prefixes modified in place.
Adjacency Table has *x* adjacencies	Total number of adjacencies.
x incomplete adjacency	Total number of incomplete adjacencies.

show cef ipv4 unresolved

To display unresolved routes in the IPv4 Cisco Express Forwarding (CEF) table, use the **show cef ipv4 unresolved** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 unresolved** [**detail**] [**hardware** {**egress**}] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
detail	(Optional) Displays detailed information unresolved routes listed in the IPv4 CEF table.
hardware	(Optional) Displays detailed information about hardware.
egress	(Optional) Displays egress packets.
location *node-id*	(Optional) Displays the unresolved routes in the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the unresolved routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 unresolved** command when an unresolved route is detected:

```
Router# show cef ipv4 unresolved

Prefix              Next Hop            Interface
10.3.3.3              102.2.2.2                ?
```

This table describes the significant fields shown in the display.

Table 17: show cef ipv4 unresolved Command Field Descriptions

Field	Description
Prefix	Prefix of the unresolved CEF.
Next Hop	Next hop of the unresolved CEF.
Interface	Next hop interface. A question mark (?) indicates that the interface has not been resolved.

show cef ipv6 adjacency

To display Cisco Express Forwarding (CEF) IPv6 adjacency status and configuration information, use the **show cef ipv6 adjacency** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 adjacency** [*interface-type interface-path-id*] [**location** *node-id*] [**detail**] [**discard**] [**glean**] [**null**] [**punt**] [**remote**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface MgmtEth0/RP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
detail	(Optional) Displays the detailed adjacency information.
discard	(Optional) Filters out and displays only the discarded adjacency information.
glean	(Optional) Filters out and displays only the glean adjacency information.
null	(Optional) Filters out and displays only the null adjacency information.
punt	(Optional) Filters out and displays only the punt adjacency information.
remote	(Optional) Filters out and displays only the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the CEF adjacency table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

show cef ipv6 adjacency hardware

To display Cisco Express Forwarding (CEF) IPv6 adjacency hardware status and configuration information, use the **show cef ipv6 adjacency hardware** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 adjacency hardware** {**egress**} [**detail** | **discard** | **drop** | **glean** | **location** *node-id* | **null** | **punt** | **remote**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
egress	Displays information from the egress packets.
detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
remote	(Optional) Displays the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 adjacency hardware** command:

```
Router#  sh cef ipv6 adjacency hardware egress location 0/6/CPU

Display protocol is ipv6
Interface    Address                                         Type    Refcount

BE31                                                         special 2
             Interface: BE31 Type:  glean
             Interface Type: 0x1c, Base Flags: 0x8001100
             Nhinfo PT: 0x9420ebb0, Idb PT: 0x93793f00, If Handle: 0xf00001c
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:44.108

 Show-data Print at RPLC




BE31          Prefix: 45:31::5/128                           local   3
             Adjacency: PT:0x91369078 45:31::5/128
             Interface: BE31
             NHID: 0x0
             MAC: 78.d3.62.4d.c5.03.78.4a.33.fd.49.03.86.dd
             Interface Type: 0x1c, Base Flags: 0x8000001
             Nhinfo PT: 0x987610b0, Idb PT: 0x93793f00, If Handle: 0xf00001c
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:37:20.035

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 693
  engctx: 0x3098761140



BE31          Prefix: fe80::7ad3:62ff:fe4d:c503/128          local   3
             Adjacency: PT:0x913692d8 fe80::7ad3:62ff:fe4d:c503/128
             Interface: BE31
             NHID: 0x0
             MAC: 78.d3.62.4d.c5.03.78.4a.33.fd.49.03.86.dd
             Interface Type: 0x1c, Base Flags: 0x8000001
             Nhinfo PT: 0x98761340, Idb PT: 0x93793f00, If Handle: 0xf00001c
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:37:20.063

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 697
  engctx: 0x30987613d0


BE31.1                                                       special 2
```

```
             Interface: BE31.1 Type:  glean
             Interface Type: 0x19, Base Flags: 0x8001100
             Nhinfo PT: 0x9420ee38, Idb PT: 0x93794290, If Handle: 0xf000024
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:44.132

 Show-data Print at RPLC




BE31.1        Prefix: 45:31:1::5/128                         local   3
             Adjacency: PT:0x91369408 45:31:1::5/128
             Interface: BE31.1
             NHID: 0x0
             MAC: 78.d3.62.4d.c5.03.78.4a.33.fd.49.03.81.00.00.01.86.dd
             Interface Type: 0x19, Base Flags: 0x8000001
             Nhinfo PT: 0x987615d0, Idb PT: 0x93794290, If Handle: 0xf000024
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:37:33.401

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 700
  engctx: 0x3098761660



BE31.1        Prefix: fe80::7ad3:62ff:fe4d:c503/128          local   3
             Adjacency: PT:0x91369668 fe80::7ad3:62ff:fe4d:c503/128
             Interface: BE31.1
             NHID: 0x0
             MAC: 78.d3.62.4d.c5.03.78.4a.33.fd.49.03.81.00.00.01.86.dd
             Interface Type: 0x19, Base Flags: 0x8000001
             Nhinfo PT: 0x98761af0, Idb PT: 0x93794290, If Handle: 0xf000024
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:37:33.414

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 705
  engctx: 0x3098761b80



FH0/0/0/6                                                    special 2
             Interface: FH0/0/0/6 Type:  glean
             Interface Type: 0xcb, Base Flags: 0x8001100
             Nhinfo PT: 0x9420e6a0, Idb PT: 0x93793320, If Handle: 0xf0001c8
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.113
 Show-data Print at RPLC



FH0/0/0/6     Prefix: 20::2/128                              local   3
             Adjacency: PT:0x913698c8 20::2/128
             Interface: FH0/0/0/6
             NHID: 0x0
             MAC: 78.1a.ee.b6.f0.00.78.4a.33.fd.48.30.86.dd
             Interface Type: 0xcb, Base Flags: 0x8000001
             Nhinfo PT: 0x98762010, Idb PT: 0x93793320, If Handle: 0xf0001c8
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:39:48.833

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 709
  engctx: 0x30987620a0



FH0/0/0/6     Prefix: fe80::7a1a:eeff:feb6:f000/128          local   3
             Adjacency: PT:0x91369b28 fe80::7a1a:eeff:feb6:f000/128
             Interface: FH0/0/0/6
             NHID: 0x0
             MAC: 78.1a.ee.b6.f0.00.78.4a.33.fd.48.30.86.dd
             Interface Type: 0xcb, Base Flags: 0x8000001
             Nhinfo PT: 0x98762530, Idb PT: 0x93793320, If Handle: 0xf0001c8
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:39:53.830

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 714
  engctx: 0x30987625c0



Hu0/0/0/32                                                   special 2
             Interface: Hu0/0/0/32 Type:  glean
             Interface Type: 0x49, Base Flags: 0x8001100
             Nhinfo PT: 0x9420dc80, Idb PT: 0x93793878, If Handle: 0xf000218
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.097

 Show-data Print at RPLC




Hu0/0/0/31                                                   special 2
             Interface: Hu0/0/0/31 Type:  glean
             Interface Type: 0x49, Base Flags: 0x8001100
             Nhinfo PT: 0x9420d9f8, Idb PT: 0x93793910, If Handle: 0xf000220
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.097

 Show-data Print at RPLC




Hu0/0/0/30                                                   special 2
             Interface: Hu0/0/0/30 Type:  glean
             Interface Type: 0x49, Base Flags: 0x8001100
             Nhinfo PT: 0x9420d770, Idb PT: 0x937939a8, If Handle: 0xf000228
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.090

 Show-data Print at RPLC




Hu0/0/0/30.1                                                 special 2
             Interface: Hu0/0/0/30.1 Type:  glean
             Interface Type: 0x19, Base Flags: 0x8001100
             Nhinfo PT: 0x9420df08, Idb PT: 0x93793f98, If Handle: 0xf000258
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.100

 Show-data Print at RPLC




Hu0/0/0/31.1                                                 special 2
             Interface: Hu0/0/0/31.1 Type:  glean
             Interface Type: 0x19, Base Flags: 0x8001100
             Nhinfo PT: 0x9420e190, Idb PT: 0x93794030, If Handle: 0xf000260
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.104

 Show-data Print at RPLC




Hu0/0/0/32.1                                                 special 2
             Interface: Hu0/0/0/32.1 Type:  glean
             Interface Type: 0x19, Base Flags: 0x8001100
             Nhinfo PT: 0x9420e418, Idb PT: 0x937940c8, If Handle: 0xf000268
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.107

 Show-data Print at RPLC




FH0/0/0/6.1                                                  special 2
```

```
             Interface: FH0/0/0/6.1 Type:  glean
             Interface Type: 0x19, Base Flags: 0x8001100
             Nhinfo PT: 0x9420e928, Idb PT: 0x93794160, If Handle: 0xf000270
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  4 22:49:42.114

 Show-data Print at RPLC




FH0/0/0/6.1   Prefix: 20:0:1::2/128                          local   3
             Adjacency: PT:0x91369d88 20:0:1::2/128
             Interface: FH0/0/0/6.1
             NHID: 0x0
             MAC: 78.1a.ee.b6.f0.00.78.4a.33.fd.48.30.81.00.00.01.86.dd
             Interface Type: 0x19, Base Flags: 0x8000001
             Nhinfo PT: 0x98762a50, Idb PT: 0x93794160, If Handle: 0xf000270
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:39:57.518

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 718
  engctx: 0x3098762ae0



FH0/0/0/6.1   Prefix: fe80::7a1a:eeff:feb6:f000/128          local   3
             Adjacency: PT:0x91369fe8 fe80::7a1a:eeff:feb6:f000/128
             Interface: FH0/0/0/6.1
             NHID: 0x0
             MAC: 78.1a.ee.b6.f0.00.78.4a.33.fd.48.30.81.00.00.01.86.dd
             Interface Type: 0x19, Base Flags: 0x8000001
             Nhinfo PT: 0x98762f70, Idb PT: 0x93794160, If Handle: 0xf000270
no dependent adj
             Ancestor If Handle: 0x0
 Update time May  5 17:40:02.514

 Show-data Print at RPLC


FIB_HAL_OBJECT_NHINFO_TX:
  hal_proto: 19
  trans_id: 0
  prev_trans_id: 723
  engctx: 0x3098763000
```

show cef ipv6

To display the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6** [*interface-type interface-number* | *ipv6-prefix/ prefix-length*] [**detail**] [**location***node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
interface-type interface-number	(Optional) IPv6 prefixes going through the specified next hop interface.
ipv6-prefix/prefix-length	(Optional) Longest prefix entry in the CEF table matching the specified IPv6 prefix and prefix length.
detail	(Optional) Displays detailed IPv6 CEF table information.
location *node-id*	(Optional) Displays the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the IPv6 CEF table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6** command:

```
Router# show cef ipv6

::/0
drop default handler
fe80::/10
receive
ff02::/16
```

```
receive
ff02::2/128
receive
ff02::1:ff00:0/104
receive
ff05::/16
receive
ff12::/16
receive
```

This table describes the significant fields shown in the display.

Table 18: show cef ipv6 Command Field Descriptions

Field	Description
drop	Indicates that packets sent to the destination prefix are dropped.
loopback	Indicates that the prefix points to a loopback address. Packets sent to loopback addresses are dropped.
receive	Indicates that the prefix is configured on one of the router interfaces. Packets sent to those prefixes are received by the router.
connected	Indicates that the prefix points to a directly connected next-hop interface.
recursive	Indicates that the prefix is not directly connected but is reachable through the next-hop prefix displayed.

The following sample output is from the **show cef ipv6** with the **detail** keyword:

```
Router# show cef ipv6 detail


::/0, version 0, proxy default, default route handler, drop adjacency, internal 0x1001011
0x0 (ptr 0x8d7d52dc) [1], 0x0 (0x8db46098), 0x0 (0x0)
Updated Nov 22 22:57:58.580
Prefix Len 0, traffic index 0, precedence n/a, priority 15
via ::/128, 3 dependencies, weight 0, class 0 [flags 0x0]
path-idx 0 NHID 0x0 [0x8cf1c218 0x0]
next hop ::/128
drop adjacency
::ffff:90.0.0.1/128, version 14, attached, receive
Updated Nov 25 15:28:03.320
Prefix Len 128
internal 0x1004141 (ptr 0x8d7d48b4) [1], 0x0 (0x8db462c8), 0x0 (0x0)
fe80::/10, version 0, receive
Updated Nov 22 22:57:58.611
Prefix Len 10
internal 0x1004001 (ptr 0x8d7d4cc4) [1], 0x0 (0x8db461e8), 0x0 (0x0)
ff02::/16, version 0, receive
Updated Nov 22 22:57:58.611
Prefix Len 16
internal 0x1004001 (ptr 0x8d7d4f14) [1], 0x0 (0x8db46140), 0x0 (0x0)
ff02::2/128, version 0, receive
Updated Nov 22 22:57:58.611
Prefix Len 128
internal 0x1004001 (ptr 0x8d7d4fe4) [1], 0x0 (0x8db46108), 0x0 (0x0)
ff02::1:ff00:0/104, version 0, receive
Updated Nov 22 22:57:58.601
```

```
Prefix Len 104
internal 0x1004001 (ptr 0x8d7d520c) [1], 0x0 (0x8db460d0), 0x0 (0x0)
ff05::/16, version 0, receive
Updated Nov 22 22:57:58.607
Prefix Len 16
internal 0x1004001 (ptr 0x8d7d513c) [1], 0x0 (0x8db461b0), 0x0 (0x0)
ff12::/16, version 0, receive
Updated Nov 22 22:57:58.607
Prefix Len 16
internal 0x1004001 (ptr 0x8d7d4d94) [1], 0x0 (0x8db46178), 0x0 (0x0)
```

This table describes the significant output fields shown in the display.

Table 19: show cef ipv6 detail Command Field Descriptions

Field	Description
flags:	Properties of the indicated prefix.
Loadinfo owner:	Owner of the Loadinfo used by the prefix for forwarding. The Loadinfo owner is the prefix that owns the array of pointers to adjacencies.
fast adj:	Cached adjacency used for forwarding.
path 1:	The following three items are displayed below path 1: • flags–Properties of the path. • next hop–Next-hop prefix if the packet is being forwarded. • interface–Next-hop interface if the packet is being forwarded.

show cef ipv6 drops

To display IPv6 Cisco Express Forwarding (CEF) table packet drop counters, use the **show cef ipv6 drops** command in XR EXEC mode.

show cef [**vrf** *vrf-name*]**ipv6 drops** [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
location *node-id*	(Optional) Displays IPv6 CEF table packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A packet might be dropped by the IPv6 CEF table because of unresolved CEF entries, unsupported features, absence of route information, absence of adjacency information, or an IP checksum error.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the packet drops for all nodes.

Note Because no hardware forwarding occurs on the route processor (RP), no packet drop information is displayed for that node.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 drops** command:

```
Router# show cef ipv6 drops location 0/RP0/CPU0

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops     packets :               0
  Unsupported drops    packets :               0
  Null0 drops          packets :               0
  No route drops       packets :               1
  No Adjacency drops   packets :              0
  Checksum error drops packets :              0
  RPF drops            packets :              0
  RPF suppressed drops packets :              0
  RP destined drops    packets :              0
  Discard drops        packets :              0
  GRE lookup drops     packets :              0
  GRE processing drops packets :              0
  LISP punt drops      packets :              0
  LISP encap err drops packets :              0
  LISP decap err drops packets :              0
```

Table 20: show cef ipv6 drops Command Field Descriptions

Field	Description
Unresolved drops	Drops due to unresolved routes.
Unsupported drops	Drops due to an unsupported feature.
Null0 drops	Drops to the Null0 interface.
No route drops	Number of packets dropped because there were no routes to the destination.
No Adjacency drops	Number of packets dropped because there were no adjacencies established.
Checksum error drops	Drops due to IPv6 checksum error.
RPF drops	Drops due to IPv6 unicast RPF[6].
RPF suppressed drops	Drops suppressed due to IPv6 unicast RPF.
RP destined drops	Drops destined for the router.
Discard drops	Drops those were discarded
GRE lookup drops	GRE packets dropped during GRE Lookup.
GRE processing drops	GRE packets dropped during GRE Processing.
LISP punt drops	LISP packets dropped during software processing of the packets.
LISP encap err drops	LISP encap packets dropped due to errors.
LISP decap err drops	LISP Decap packets dropped due to errors.

[6] RPF = Reverse Path Forwarding

show cef ipv6 exact-route

To display the path an IPv6 flow comprising a source and destination address would take, use the **show cef ipv6 exact-route** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 exact-route** { *source-address destination-address* } [**flow-label** *flow-label-value*] [**protocol** { *protocol-number* | *protocol-value* }] [**source-port** *source-port-number*] [**destination-port** *destination-port-number*] [**ingress-interface interface-type** *interface-id*] [**hardware** { **ingress** | **egress** }] [**policy-class** *value*] [**detail | location** *node-id]*] { **ingress-interface** *ingress-interface* | **user-data** *user-data* **ingress-interface** *ingress-interface* [**brief** | **detail** | **flow-label** | **hardware** | **internal** | **location** | **policy-class** | **protocol**] }

Syntax Description

vrf	(Optional) Sets VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
source-address	The IPv6 source address in x:x::x format.
destination-address	The IPv6 destination address in x:x::x format.
protocol *protocol-number* | *protocol-name*	Sets the specified protocol for the route.
source-port *source-port-number*	(Optional) Sets the source port. The range is from 0 to 65535.
destination-port *destination-port-number*	(Optional) Sets the destination port. The range is from 0 to 65535.
ingress-interface interface-type *interface-id*	Sets the ingress interface type and ID.
hardware { **protocol-value** | **protocol-name** }	(Optional) Reads from the ingress or egress packet.
flow-label *flow-label-value*	Sets the IPv6 flow-label and flow-label-value.
policy-class *value*	(Optional) Sets the class for the policy-based tunnel selection. The range for the tunnel policy class value is from 1 to 7.
detail	(Optional) Provides full CEF entry information.

location *node-id*	(Optional) Provides the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
ingress-interface	(Optional) Specifies the ingress interface information.
user-data *user-data*	(Optional) Specifies the additional user chosen data bytes used in multi-path computation. In *user-data*, you can enter 1-4 bytes in hexadecimal.
ingress-interface *ingress-interface*	Specifies the ingress interface information.
brief	(Optional) Displays brief information of CEF table.
detail	(Optional) Displays full information of CEF table.
flow-label	(Optional) Specifies the IPv6 flow-label.
hardware	(Optional) Displays information from hardware.
location	(Optional) Provides the forwarding information for the designated node. The node-id argument is entered in the *rack/slot/module* notation.
policy-class	(Optional) Class for policy-based tunnel selection.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.5	The keyword **user-data** was introduced.
Release 24.2.11	The keyword **user-data** was introduced.
Release 7.0.12	This command was introduced.

Usage Guidelines

For TCP and UDP protocols, providing the source-port and destination-port is mandatory. For other protocols, provide the source-port and destination-port as zero. Providing flow-label is also mandatory. Otherwise, the output of the **show cef ipv6 exact-route** command is not correct.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 exact-route** command:

```
Router# show cef ipv6 exact-route 2001:DB8::1 2001:DB8:0:ABCD::1 flow-label 15000 protocol
 UDP source-port 34000 destination-port 45000 ingress-interface HundredGigE 0/0/0/24
Wed Apr 15 02:36:17.632 UTC
2001:DB8:0:ABCD::1/128, version 27, labeled SR, internal 0x1000001 0x8010 (ptr 0x96a0571c)
 [1], 0x0 (0x969e5160), 0xa28 (0x9849c120)
 Updated Apr 14 21:29:19.925
 local adjacency fe80::7ace:ecff:fecf:d103
 Prefix Len 128, traffic index 0, precedence n/a, priority 1, encap-id 0x1001500000001
   via Bundle-Ether2
   via fe80::7ace:ecff:fecf:d103/128, Bundle-Ether2, 7 dependencies, weight 0, class 0
[flags 0x0]
    path-idx 0 NHID 0x0 [0x981225d0 0x0]
    next hop fe80::7ace:ecff:fecf:d103/128
     local adjacency
     local label 21556 labels imposed {21556}
```

The following sample output is from the **show cef ipv6 exact-route** command with **user-data** keyword:

```
Router# show cef ipv6 exact-route 100::10 60::1 flow-label 0 protocol 59 source-port 0
destination-port 0 user-data 0x2 ingress-interface HundredGigE0/0/0/2 location 0/0/cpu0

Unsupported protocol value 59
60::/16, version 1293, internal 0x1000001 0x20 (ptr 0x8b78ef00) [1], 0x400 (0x8e9cfc48),
0x0 (0x0)
 Updated Aug 14 07:50:20.022
 local adjacency to Bundle-Ether3.30

 Prefix Len 16, traffic index 0, precedence n/a, priority 2
   via Bundle-Ether3.30
   via fe80::72b3:17ff:feae:d703/128, Bundle-Ether3.30, 7 dependencies, weight 0, class 0
[flags 0x0]
    path-idx 7 NHID 0x0 [0x8db8bed8 0x0]
    next hop fe80::72b3:17ff:feae:d703/128
    local adjacency
```

show cef ipv6 exceptions

To display IPv6 Cisco Express Forwarding (CEF) exception packet counters, use the **show cef ipv6 exceptions** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 exceptions** [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
location *node-id*	(Optional) Displays IPv6 CEF exception packet counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

CEF exception packets are those packets that have been sent from the hardware to the software because they require additional handling. The types of IPv6 CEF exception packets are displayed in the output of **show cef ipv6 exceptions**.

If you do not specify a node with **location** keyword and *node-id* argument, this command displays IPv6 CEF exception packet counters for all nodes.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 exceptions** command:

```
Router# show cef ipv6 exceptions location 0/RP0/CPU0

CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap  packets :             0
  Unsupported packets :             0
  Redirect    packets :             0
  Receive     packets :             1
  Broadcast   packets :             0
  IP options  packets :             0
  TTL expired packets :             0
  Fragmented  packets :             0
```

show cef ipv6 hardware

To display Cisco Express Forwarding (CEF) IPv6 hardware status and configuration information, use the **show cef ipv6 hardware** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 hardware** {**egress** | [**detail** | **location** *node-id*]}

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
egress	Displays information from the egress packets.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output displays the full details from the **show cef ipv6 hardware** command:

```
Router# show cef ipv6 hardware egress detail

::/0, version 0, proxy default, default route handler, drop adjacency, internal 0x1001011
0x0 (ptr 0x8d7d52dc) [1], 0x0 (0x8db46098), 0x0 (0x0)
Updated Nov 22 22:57:58.578
Prefix Len 0, traffic index 0, precedence n/a, priority 15
gateway array (0x8d87a098) reference count 1, flags 0x200, source default (12), 0 backups
[2 type 3 flags 0xa401 (0x8d9cf098) ext 0x0 (0x0)]
LW-LDI[type=3, refc=1, ptr=0x8db46098, sh-ldi=0x8d9cf098]
gateway array update type-time 1 Nov 22 22:57:58.578
LDI Update time Nov 22 22:57:58.595
LW-LDI-TS Nov 22 22:57:58.595
via ::/128, 3 dependencies, weight 0, class 0 [flags 0x0]
path-idx 0 NHID 0x0 [0x8cf1c218 0x0]
```

```
next hop ::/128
drop adjacency


Load distribution: 0 (refcount 2)

Hash OK Interface Address
0 Y Unknown drop
::ffff:90.0.0.1/128, version 14, attached, receive
Updated Nov 25 15:28:03.318
Prefix Len 128
internal 0x1004141 (ptr 0x8d7d48b4) [1], 0x0 (0x8db462c8), 0x0 (0x0)
fe80::/10, version 0, receive
Updated Nov 22 22:57:58.608
Prefix Len 10
internal 0x1004001 (ptr 0x8d7d4cc4) [1], 0x0 (0x8db461e8), 0x0 (0x0)
ff02::/16, version 0, receive
Updated Nov 22 22:57:58.609
Prefix Len 16
internal 0x1004001 (ptr 0x8d7d4f14) [1], 0x0 (0x8db46140), 0x0 (0x0)
```

show cef ipv6 interface

To display IPv6 Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef ipv6 interface** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 interface** *type interface-path-id* [**detail**] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
location *node-id*	(Optional) Displays IPv4 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef ipv6 interface** command displays the CEF-related information for the interface on the route processor.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef ipv6 interface HundredGigE 0/0/0/0** command:

```
Router# show cef ipv6 interface HundredGigE 0/0/0/0

HundredGigE0/0/0/0 is up if_handle 0x0f000138 if_type IFT_HUNDREDGE(0x49)
     idb info 0x9093e730 flags 0x8001 ext 0x9557d0a8 flags 0x50
```

```
   Vrf Local Info (0x95b7a0a8)
Interface last modified Jan 13, 2020 06:08:29, create
Reference count 1       Next-Hop Count 1
Forwarding is enabled
ICMP redirects are never sent
ICMP unreachables are enabled
Protocol MTU 1500, TableId 0xe0800000(0x91382758)
Protocol Reference count 2
Primary IPV6 local address 100::6/128
```

show cef ipv6 non-recursive

To display the IPv6 nonrecursive prefix entries in the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 non-recursive** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 non-recursive** [**hardware** {**egress** | **ingress**}] [**detail**] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
hardware	(Optional) Displays Cisco Express Forwarding (CEF) IPv6 hardware status and configuration information.
egress	(Optional) Displays information from the egress packets.
ingress	(Optional) Displays information from the ingress packets.
detail	(Optional) Displays full details.
location *node-id*	(Optional) Displays the nonrecursive prefix entries in the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the nonrecursive routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 non-recursive** command:

```
Router# show cef ipv6 non-recursive

20::/64
connected FourHundredGigE0/0/0/6
20::2/128
20::2/128 FourHundredGigE0/0/0/6
20::3/128
```

```
receive FourHundredGigE0/0/0/6
20:0:1::/64
connected FourHundredGigE0/0/0/6.1
20:0:1::2/128
20:0:1::2/128 FourHundredGigE0/0/0/6.1
20:0:1::3/128
receive FourHundredGigE0/0/0/6.1
30:30::/64
connected HundredGigE0/0/0/30
30:30::3/128
receive HundredGigE0/0/0/30
30:30:1::/64
connected HundredGigE0/0/0/30.1
30:30:1::3/128
receive HundredGigE0/0/0/30.1
30:31::/64
connected HundredGigE0/0/0/31
30:31::3/128
receive HundredGigE0/0/0/31
30:31:1::/64
connected HundredGigE0/0/0/31.1
30:31:1::3/128
receive HundredGigE0/0/0/31.1
30:32::/64
connected HundredGigE0/0/0/32
30:32::3/128
receive HundredGigE0/0/0/32
30:32:1::/64
connected HundredGigE0/0/0/32.1
30:32:1::3/128
receive HundredGigE0/0/0/32.1
45:31::/64
connected Bundle-Ether31
45:31::3/128
receive Bundle-Ether31
45:31::5/128
45:31::5/128 Bundle-Ether31
45:31:1::/64
connected Bundle-Ether31.1
45:31:1::3/128
receive Bundle-Ether31.1
45:31:1::5/128
45:31:1::5/128 Bundle-Ether31.1
210:210:1::3/128
receive Loopback0
```

This table describes the significant fields shown in the display.

Table 21: show cef ipv6 non-recursive Command Field Descriptions

Field	Description
drop	Indicates that packets sent to the destination prefix are dropped.
loopback	Indicates that the prefix points to a loopback address. Packets sent to loopback addresses are dropped.
receive	Indicates that the prefix is configured on one of the router interfaces. Packets sent to those prefixes are received by the router.
connected	Indicates that the prefix points to a directly connected next-hop interface.

show cef ipv6 resource

To display the IPv6 nonrecursive prefix entries in the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 resource** command in XR EXEC mode.

show cef ipv6 resource [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed information resources listed in the IPv6 CEF table.
location *node-id*	(Optional) Displays the IPv6 resource entries in the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the output displays the IPv6 CEF nonrecursive routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 resource** command:

```
Router# show cef ipv6 resource

CEF resource availability summary state: GREEN
  ipv4 shared memory resource: GREEN
  ipv6 shared memory resource: GREEN
  mpls shared memory resource: GREEN
  common shared memory resource: GREEN
  TABLE hardware resource: GREEN
  LEAF hardware resource: GREEN
  LOADINFO hardware resource: GREEN
  NHINFO hardware resource: GREEN
  LABEL_INFO hardware resource: GREEN
  IDB hardware resource: GREEN
  FRR_NHINFO hardware resource: GREEN
  LDSH_ARRAY hardware resource: GREEN
  RSRC_MON hardware resource: GREEN
```

show cef ipv6 summary

To display a summary of the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 summary** command in XR EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 summary** [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
location *node-id*	(Optional) Displays a summary of the IPv6 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays a summary of the IPv6 CEF table for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 summary** command:

```
Router# show cef ipv6 summary

IP CEF with switching (Table Version 0)

  Load balancing: L3
  Tableid 0xe0800000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
  Vrfname default, Refcount 12
  4 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 288 bytes
  0 load sharing elements, 0 bytes, 0 references
  0 shared load sharing elements, 0 bytes
  0 exclusive load sharing elements, 0 bytes
  0 CEF route update drops, 0 revisions of existing leaves
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  0 prefixes with label imposition, 0 prefixes with label information
Adjacency Table has 44 adjacencies
  1 incomplete adjacency
```

This table describes the significant fields shown in the display.

Table 22: show cef ipv6 summary Command Field Descriptions

Field	Description
Load balancing	Current load-balancing mode. The default value is L3.
Table Version	Version of the CEF table.
routes	Total number of routes.
unresolved (*x* old, *x* new)	Number of routes not yet resolved.
load sharing elements	Total number of internal load-sharing data structures.
bytes	Total memory used by internal load sharing data structures.
references	Total reference count of all internal load sharing data structures.
CEF resets	Number of CEF table resets.
revisions of existing leaves	Number of updates to existing prefixes.
Exponential (currently *x*s, peak *x*s)	Currently not used.
prefixes modified in place	Prefixes modified in place.
Router ID	Router identification.
Adjacency Table has *x* adjacencies	Total number of adjacencies.
x incomplete adjacency	Total number of incomplete adjacencies.

show cef ipv6 unresolved

To display the unresolved routes in the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6 unresolved** command in XR EXEC mode.

show **cef** [**vrf** *vrf-name*] **ipv6** **unresolved** [**detail**] [**hardware** {**egress**}] [**location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
detail	(Optional) Displays full details.
hardware	(Optional) Displays Cisco Express Forwarding (CEF) IPv6 hardware status and configuration information.
egress	Displays information from the egress packets.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the unresolved routes for the node on which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef ipv6 unresolved** command when an unresolved route is detected:

```
Router# show cef ipv6 unresolved

9999::/64
  unresolved
```

This table describes the significant fields shown in the display.

Table 23: show cef ipv6 unresolved Command Field Descriptions

Field	Description
xxxx::/*xx*	Detected unresolved route.

show cef mpls adjacency

To display the Multiprotocol Label Switching (MPLS) adjacency table, use the **show cef mpls adjacency** command in XR EXEC mode.

show cef mpls adjacency [*interface-type interface-path-id*] [**detail** | **discard** | **drop** | **glean** | **null** | **punt** | **remote**] [**location** *node-id*]

Syntax Description

interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface- path-id	(Optional) Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash mark between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface MgmtEth0/RP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
remote	(Optional) Displays the remote adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef mpls adjacency** command displays the MPLS adjacency table for the node in which the command is issued.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef mpls adjacency** command:

```
Router# sh cef mpls adjacency inter

Display protocol is mpls
Interface    Address                                        Type   Refcount

BE1906       Prefix: 10.0.86.1/32                           local   7
             Adjacency: PT:0x8cba28d0 10.0.86.1/32
             Interface: BE1906
             NHID: 0x0
             MAC: e6.48.5c.10.b4.8e.e6.07.2b.8d.34.88.88.47
             Interface Type: 0x1c, Base Flags: 0x1 (0x8d10f620)
             Nhinfo PT: 0x8d10f620, Idb PT: 0x8ca57320, If Handle:
0x8000174
no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec 21 03:56:49.977


BE1904       Prefix: 10.0.85.1/32                           local   7
             Adjacency: PT:0x8cba3c78 10.0.85.1/32
             Interface: BE1904
             NHID: 0x0
             MAC: e6.48.5c.10.b4.86.e6.07.2b.8d.34.89.88.47
             Interface Type: 0x1c, Base Flags: 0x1 (0x8d10f1a0)
             Nhinfo PT: 0x8d10f1a0, Idb PT: 0x8ca572a0, If Handle:
0x800016c
no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec 21 03:57:25.360
```

show cef mpls adjacency hardware

To display the Multiprotocol Label Switching (MPLS) adjacency hardware status and configuration information, use the **show cef mpls adjacency hardware** command in XR EXEC mode.

show cef mpls adjacency hardware {**egress**} [**detail** | **discard** | **drop** | **glean** | **location** *node-id* | **null** | **punt** | **remote**]

Syntax Description

egress	Displays information from the egress packets.
detail	(Optional) Displays full details.
discard	(Optional) Displays the discard adjacency information.
drop	(Optional) Displays the drop adjacency information.
glean	(Optional) Displays the glean adjacency information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
null	(Optional) Displays the null adjacency information.
punt	(Optional) Displays the punt adjacency information.
remote	(Optional) Displays the remote adjacency information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef mpls adjacency hardware** command:

```
Router# sh cef mpls adjacency inter

Display protocol is mpls
Interface    Address                                          Type   Refcount
```

```
BE1906       Prefix: 10.0.86.1/32                            local   7
             Adjacency: PT:0x8cba28d0 10.0.86.1/32
             Interface: BE1906
             NHID: 0x0
             MAC: e6.48.5c.10.b4.8e.e6.07.2b.8d.34.88.88.47
             Interface Type: 0x1c, Base Flags: 0x1 (0x8d10f620)
             Nhinfo PT: 0x8d10f620, Idb PT: 0x8ca57320, If Handle:
0x8000174
no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec 21 03:56:49.977


BE1904       Prefix: 10.0.85.1/32                            local   7
             Adjacency: PT:0x8cba3c78 10.0.85.1/32
             Interface: BE1904
             NHID: 0x0
             MAC: e6.48.5c.10.b4.86.e6.07.2b.8d.34.89.88.47
             Interface Type: 0x1c, Base Flags: 0x1 (0x8d10f1a0)
             Nhinfo PT: 0x8d10f1a0, Idb PT: 0x8ca572a0, If Handle:
0x800016c
no dependent adj
             Ancestor If Handle: 0x0
 Update time Dec 21 03:57:25.360
```

show cef mpls drops

To display Multiprotocol Label Switching (MPLS) drop counters for packets that belong to a segment routing (SR) network, use the **show cef mpls drops** command in XR EXEC mode.

show cef mpls drops [**location** {*node-id* | **all**}]

Syntax Description

location *node-id*	(Optional) Displays detailed Cisco Express Forwarding (CEF) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	(Optional) Displays all locations.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to display the SR MPLS drop counters.

The incoming top MPLS label is inspected. If the label belongs to the Segment Routing Local Block (SRLB) or the Segment Routing Global Block (SRGB), an MPLS SR drop counter is incremented for unknown label value or for MPLS time to live (TTL) expiry.

Note The drop counters will increment for manually allocated adjacency SIDs and prefix SIDs only. They will not increment for dynamically allocated adjacency SIDs.

Task ID

Task ID	Operation
cef	read

Example

This following is sample output from **show cef mpls drops** command:

```
Router# show cef mpls drops location 0/0/CPU0
Sat Jun  9 03:49:27.100 IST
CEF Drop Statistics
Node: 0/0/CPU0
  SR MPLS unreachable packets :               100
  SR MPLS TTL expired packets :               400
```

show cef mpls interface

To display the Multiprotocol Label Switching (MPLS) Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef mpls interface** command in XR EXEC mode.

show cef mpls interface *type* *interface-path-id* [**detail**] [**location** *node-id*]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
in terface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0) and the module is CPU0. Example: interface MgmtEth0/ RP0 • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
location *node-id*	(Optional) Displays IPv4 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you do not specify a node with the **location** keyword and *node-id* argument, the **show cef mpls interface** command displays the CEF-related information for the interface on the route processor.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef mpls interface** command:

```
Router#  sh cef mpls interface hundredGigE 0/0/0/24
Wed Apr 22 16:56:48.376 UTC
HundredGigE0/0/0/24 is down if_handle 0x0f0001f8 if_type IFT_HUNDREDGE(0x49)
     idb info 0x912e6ae0 flags 0x8001 ext 0x0
     Vrf Local Info (0x0)
  Interface last modified Apr 22, 2020 14:28:51, create
  Reference count 1       Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
```

show cef mpls unresolved

To display the Multiprotocol Label Switching (MPLS) unresolved routes, use the **show cef mpls unresolved** command in XR EXEC mode.

show cef mpls unresolved [**detail**] [**location** *node-id*]

Syntax Description

detail	(Optional) Displays detailed adjacency information, including Layer 2 information.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef mpls unresolved** command:

```
Router# show cef mpls unresolved

Label/EOS           Next Hop            Interface
20001/0
20001/1
```

This table describes the significant fields shown in the display.

Table 24: show cef mpls unresolved Command Field Descriptions

Field	Description
Label/EOS	MPLS forwarding label/End of Stack (EOS) bit.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

show cef recursive-nexthop

To display Cisco Express Forwarding (CEF) recursive next-hop information, use the**show cef recursive-nexthop** command in XR EXEC mode.

show cef recursive-nexthop [**hardware**] [**location node-id**]

Syntax Description

hardware	(Optional) Displays hardware information related to the recursive next hop.
location *node-id*	(Optional) Displays recursive next-hop information for the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Related Commands

Command	Description
show cef, on page 162	Displays information about packets forwarded by Cisco Express Forwarding (CEF).

show cef summary

To display summary information for the Cisco Express Forwarding (CEF) table, use the **show cef summary** command in XR EXEC mode.

show cef summary [**location** {*node-id* | **all**}]

Syntax Description

location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	(Optional) Displays all locations.

Command Default

The **show cef summary** command assumes the IPv4 CEF table and the active RP node as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
cef	read

Examples

The following sample output is from the **show cef summary** command.

```
Router# show cef summary location 0/RP0/CPU0

Router ID is 10.1.1.1

IP CEF with switching (Table Version 0) for node0_1_CPU0

  Load balancing: L3
  Tableid 0xe0000000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
  Vrfname default, Refcount 318
  170 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 12240 bytes
  183 load sharing elements, 57292 bytes, 184 references
  19 shared load sharing elements, 7036 bytes
  164 exclusive load sharing elements, 50256 bytes
  0 CEF route update drops, 10 revisions of existing leaves
  Resolution Timer: 15s
  0 prefixes modified in place
  0 deleted stale prefixes
  21 prefixes with label imposition, 60 prefixes with label information
Adjacency Table has 49 adjacencies
  25 incomplete adjacencies
```

This table describes the significant fields shown in the display.

Table 25: show cef summary Command Field Descriptions

Field	Description
Load balancing	Current load-balancing mode. The default value is L3.
Table Version	Version of the CEF table.
tableid	Table identification number.
vrfname	VRF name.
flags	Option value for the table
routes	Total number of routes.
reresolve	Total number of routes being reresolved.
unresolved (*x* old, *x* new)	Number of routes not yet resolved.
load sharing elements	Total number of internal load-sharing data structures.
bytes	Total memory used by internal load sharing data structures.
references	Total reference count of all internal load sharing data structures.
CEF resets	Number of CEF table resets.
revisions of existing leaves	Number of updates to existing prefixes.
Exponential (currently *x*s, peak *x*s)	Currently not used.
prefixes modified in place	Prefixes modified in place.
Adjacency Table has *x* adjacencies	Total number of adjacencies.
x incomplete adjacency	Total number of incomplete adjacencies.

show cef vrf

To display the contents of the VPN routing and forwarding (VRF) instance, use the **show cef vrf** command in XR EXEC mode.

show cef vrf [*vrf-name*]

Syntax Description

vrf-name	Name of the VRF instance.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

To display unresolved routes, you must use the **unresolved** keyword explicitly.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef vrf** command when an unresolved route is detected:

```
Router# show cef vrf test1
Tue Apr 28 04:21:48.588 UTC

Prefix              Next Hop            Interface
------------------- ------------------- ------------------
0.0.0.0/0           drop                default handler
0.0.0.0/32          broadcast
26.0.0.0/24         attached            HundredGigE0/0/0/26
26.0.0.0/32         broadcast           HundredGigE0/0/0/26
26.0.0.1/32         26.0.0.1/32         HundredGigE0/0/0/26
26.0.0.2/32         receive             HundredGigE0/0/0/26
26.0.0.255/32       broadcast           HundredGigE0/0/0/26
27.0.0.0/24         attached            HundredGigE0/0/0/27
27.0.0.0/32         broadcast           HundredGigE0/0/0/27
27.0.0.2/32         receive             HundredGigE0/0/0/27
27.0.0.3/32         27.0.0.3/32         HundredGigE0/0/0/27
27.0.0.255/32       broadcast           HundredGigE0/0/0/27
224.0.0.0/4         0.0.0.0/32
224.0.0.0/24        receive
```

This table describes the significant fields shown in the display.

Table 26: show cef vrf Command Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

show hw-module profile cef

To display information about the configuration status of CEF hardware-modules, use the **show hw-module profile cef** command in XR EXEC mode.

show hw-module profile cef

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Task ID

Task ID	Operations
cef	read

Examples

This sample output is from the **show hw-module profile cef** command:

```
Router# show hw-module profile cef
Tue Oct 6 00:34:47.735 UTC
--------------------------------------------------------------------------------------
Knob                                           Status      Applied    Action
--------------------------------------------------------------------------------------
BGPLU                                       Configured       No       Reload
Dark Bandwidth                              Unconfigured     Yes      None
MPLS Per Path Stats                         Unconfigured     Yes      None
Tunnel TTL Decrement                        Configured       Yes      None
High-Scale No-LDP-Over-TE                   Unconfigured     Yes      None
```

Host Services and Applications Commands

This chapter describes the commands used to configure and monitor the Host Services and Applications on Cisco 8000 Series Routers.

For detailed information about Host Services and Applications concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

cinetd rate-limit

To configure the rate limit at which service requests are accepted by Cisco inetd (Cinetd), use the **cinetd rate-limit** command in XR Config mode. To restore the default, use the **no** form of this command.

cinetd rate-limit *value*
no cinetd rate-limit *value*

Syntax Description

value	Number of service requests that are accepted per second. Range is 1 to 100. Default is 1.

Command Default

One service request per second is accepted.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Any service request that exceeds the rate limit is rejected. The rate limit is applied to individual applications.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows the **cinetd rate-limit** being set to 10:

```
Router# config
Router(config)# cinetd rate-limit 10
```

clear host

To delete temporary entries from the hostname-to-address cache, use the **clear host** command in XR EXEC mode.

clear host {*host-name* | *****}

Syntax Description

host-name	Name of host to be deleted.
*	Specifies that all entries in the local cache be deleted.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The dynamic host entries in the cache are cleared.

The temporary entries in the cache are cleared; the permanent entries that were entered with the `domain ipv4 host` or the `domain ipv6 host` command are not cleared.

By default, no static mapping is configured.

Task ID

Task ID	Operations
ip-services	execute

Examples

The following example shows how to clear all temporary entries from the hostname-and-address cache:

```
Router# clear host *
```

domain ipv4 host

To define a static hostname-to-address mapping in the host cache using IPv4, use the **domain ipv4 host** command in XR Config mode. To remove the **domain ipv4 host** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

domain ipv4 host *host-name v4address2......v4address8*
no domain ipv4 host *host-name v4address1*

Syntax Description

host-name	Name of the host. The first character can be either a letter or a number.
v4address1	Associated IP address.
v4address2...v4address8	(Optional) Additional associated IP address. You can bind up to eight addresses to a hostname.

Command Default

No static mapping is configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Task ID

Task ID	Operations
ip-services	read, write
basic-services	read, write

Examples

The following example shows how to define two IPv4 static mappings:

```
Router(config)# domain ipv4 host host1 192.168.7.18
Router(config)# domain ipv4 host bost2 10.2.0.2 192.168.7.33
```

domain ipv6 host

To define a static hostname-to-address mapping in the host cache using IPv6, use the **domain ipv6 host** command in XR Config mode. To remove the **domain ipv6 host** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

domain ipv6 host *host-name v6address1 [v6address2 ......v6address4]*
no domain ipv6 host *host-name v6address1*

Syntax Description

host-name	Name of the host. The first character can be either a letter or a number.
v6address1	Associated IP address.
v6address2...v6address4	(Optional) Additional associated IP address. You can bind up to four addresses to a hostname.

Command Default

No static mapping is configured. IPv6 address prefixes are not enabled.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The first character can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Task ID

Task ID	Operations
ip services	read, write

Examples

The following example shows how to define two IPv6 static mappings:

```
Router(config)# domain ipv6 host host1 ff02::2
Router(config)# domain ipv6 host host2 ff02::1
```

domain list

To define a list of default domain names to complete unqualified hostnames, use the **domain list** command in XR Config mode. To delete a name from a list, use the **no** form of this command.

domain list *domain-name*
no domain list *domain-name*

Syntax Description

domain-name	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No domain names are defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If there is no domain list, the domain name that you specified with the `domain name (IPAddr)` command is used to complete unqualified hostnames. If there is a domain list, the default domain name is not used. The **domain list** command is similar to the `domain name (IPAddr)` command, except that you can use the **domain list** command to define a list of domains, each to be tried in turn.

Task ID

Task ID	Operations
ip-service	read, write

Examples

The following example shows how to add several domain names to a list:

```
Router(config)# domain list domain1.com
Router(config)# domain list domain2.edu
```

The following example shows how to add a name to and then delete a name from the list:

```
Router(config)# domain list domain3.edu
Router(config)# no domain list domain2.edu
```

domain lookup disable

To disable the IP Domain Name System (DNS)-based hostname-to-address translation, use the **domain lookup disable** command in XR Config mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

domain lookup disable
no domain lookup disable

Syntax Description

This command has no keywords or arguments.

Command Default

The IP DNS-based host-to-address translation is enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Using the **no** command removes the specified command from the configuration file and restores the system to its default condition. The **no** form of this command is not stored in the configuration file.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to enable the IP DNS-based hostname-to-address translation:

```
Router(config)# domain lookup disable
```

domain name (IPAddr)

To define a default domain name that the software uses to complete unqualified hostnames, use the **domain name** command in the appropriate mode. To remove the name, use the **no** form of this command.

domain name *domain-name*
no domain name *domain-name*

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name.

Command Default

There is no default domain name.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If a hostname does not contain a domain name, then a dot and the domain name configured by the **domain name** command are appended to the hostname before it is added to the host table.

If no domain name is configured by the **domain name** command and the user provides only the hostname, then the request is not looked up.

Task ID

Task ID	Operations
ip-services	read, write

domain name-server

To specify the address of one or more name servers to use for name and address resolution, use the **domain name-server** command in XR Config mode. To remove the address specified, use the **no** form of this command.

domain name-server *server-address*
no domain name-server *server-address*

Syntax Description

server-address	IP address of a name server.

Command Default

If no name server address is specified, the default name server is 255.255.255.255. IPv4 and IPv6 address prefixes are not enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

You can enter up to six addresses, but only one for each command.

If no name server address is specified, the default name server is 255.255.255.255 so that the DNS lookup can be broadcast to the local network segment. If a DNS server is in the local network, it replies. If not, there might be a server that knows how to forward the DNS request to the correct DNS server.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify host 192.168.1.111 as the primary name server and host 192.168.1.2 as the secondary server:

```
Router(config)# domain name-server 192.168.1.111
Router(config)# domain name-server 192.168.1.2
```

ftp client anonymous-password

To assign a password for anonymous users, use the **ftp client anonymous-password** command in XR Config mode. To remove the **ftp client anonymous-password** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

ftp client anonymous-password *password*
no ftp client anonymous-password

Syntax Description

password	Password for the anonymous user.

Command Default

No default behavior or values

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ftp client anonymous-password** command is File Transfer Protocol (FTP) server dependent.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the anonymous password to *xxxx*:

```
Router(config)# ftp client anonymous-password xxxx
```

ftp client passive

To configure the software to use only passive File Transfer Protocol (FTP) connections, use the **ftp client passive** command in XR Config mode. To remove the **ftp client passive** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

ftp client passive
no ftp client passive

Syntax Description

This command has no keywords or arguments.

Command Default

FTP data connections are active.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Using the **ftp client passive** command allows you to make only passive-mode FTP connections. To specify the source IP address for FTP connections, use the **ftp client source-interface** command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the networking device to use only passive FTP connections:

```
Router(config)# ftp client passive

1d:3h:54:47: ftp_fs[16437]: FTP: verifying tuple passive (SET).
1d:3h:54:47: ftp_fs[16437]: FTP: applying tuple passive (SET).
1d:3h:54:47: ftp_fs[16437]: FTP: passive mode has been enabled.
```

ftp client password

To specify the password for the File Transfer Protocol (FTP) connections, use the **ftp client password** command in XR Config mode. To disable this feature, use the **no** form of this command.

ftp client password {*clear-text-password* | **clear** *clear-text password* | **encrypted** *encrypted-text password*}
no ftp client password {*clear-text-password* | **clear** *clear-text password* | **encrypted** *encrypted-text password*}

Syntax Description

clear-text-password	Specifies an unencrypted (cleartext) user password
clear *clear-text password*	Specifies an unencrypted (cleartext) shared password.
encrypted *encrypted-text password*	Specifies an encrypted shared password.

Command Default

No default behavior or values

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify the password for the File Transfer Protocol (FTP) connections:

```
Router(config)# ftp client password lab
```

ftp client source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ftp client source-interface** command in XR Config mode . To remove the **ftp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

ftp client source-interface *type interface-path-id*
no ftp client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The FTP source address is the IP address of the interface used by the FTP packets to leave the networking device.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to set the same source address for all FTP connections. To configure the software to use only passive FTP connections, use the **ftp client passive** command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the IP address associated with HundredGigEinterface 0/1/2/1 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
Router(config)# ftp client source-interface HundredGigE0/1/2/1
```

ftp client username

To specify the username for File Transfer Protocol (FTP) connections, use the **ftp client username** command in XR Config mode. To disable this feature, use the **no** form of this command.

ftp client username *username*
no ftp client username *username*

Syntax Description

username	Name for FTP user.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to specify the username for FTP connections:

```
Router(config)# ftp client username brownfox
```

http client connection

To configure the connection for http client, use the **http client connection** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client connection { **retry** *count* | **timeout** *seconds* }

Syntax Description

retry *count*	Specifies how many times HTTP Client resends a connection request. Range is from 1 to 5. The default value is 0.
timeout *seconds*	The time interval (in seconds) that HTTP client waits for a server connection to establish before giving up. Range is from 1 to 60 seconds. The default value is 10 seconds.

Command Default

The connection retry is not configured by default. The default connection timeout is set to 10 seconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to set the connection timeout or connection retry count.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the connection request retry to two times:

```
RP/0/RP0/CPU0:router(config)#http client connection retry 2
```

The following example shows how to configure the connection request timeout to 20 seconds:

```
RP/0/RP0/CPU0:router(config)#http client connection timeout 20
```

http client response

To configure the time interval (in seconds) for HTTP Client to wait for a response from the server before giving up, use the **http client response** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client response { **timeout** *seconds* }

Syntax Description

timeout *seconds*	The time interval (in seconds) that HTTP client waits for a response from the server before giving up. Range is from 1 to 300 seconds. The default value is 30 seconds.

Command Default

The response timeout is 30 seconds by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to configure the response timeout.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the response timeout to 40 seconds:

```
RP/0/RP0/CPU0:router(config)#http client response timeout 40
```

http client secure-verify-host

To enable verifying host in peer's certificate, use the **http client secure-verify-host** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client secure-verify-host

Syntax Description

secure-verify-host	Verifies the host in peer's certificate. This is enabled by default. To disable, use the command **http client secure-verify-host** *disable*

Command Default

Host verification is enabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **http client secure-verify-host** command to disable the host verification.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to disable host verification :

```
RP/0/RP0/CPU0:router(config)#http client secure-verify-host disable
```

http client secure-verify-peer

To enable verifying authenticity of the peer certificate, use the **http client secure-verify-peer** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client secure-verify-peer

Syntax Description

secure-verify-peer	Verifies authenticity of the peer certificate. This is enabled by default. To disable, use the command **http client secure-verify-peer** *disable*

Command Default

Peer verification is enabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **http client secure-verify-peer** command to disable the peer verification.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to disable peer verification :

```
RP/0/RP0/CPU0:router(config)#http client secure-verify-peer disable
```

http client source-interface

To specify the interface for source address for Hypertext Transfer Protocol (HTTP) connections, use the **http client source-interface** command in XR Config mode. To remove the **http client source-interface**command from the configuration file and restore the system to its default condition, use the **no** form of this command.

http client source-interface { **ipv4** | **ipv6** }

Syntax Description

ipv4 *ip-address*	Enter ipv4 address from interface.
ipv6 *ip-address*	Enter ipv6 address from interface.

Command Default

No default behavior or values.

Command History

Release	Modification
Release 7.10.1	This command was modified to configure both ipv4 and ipv6 source interfaces.
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **http client source-interface** command to configure ipv4 and ipv6 source interfaces. If both the source interfaces are configured, then the source interface is selected depending on the host DNS resolution.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure ipv4 source interface for HTTP connection:

```
RP/0/RP0/CPU0:router(config)#http client source-interface ipv4 gigabitEthernet 0/0/0/0
```

The following example shows how to configure ipv6 source interface for HTTP connection:

```
RP/0/RP0/CPU0:router(config)#http client source-interface ipv6 gigabitEthernet 0/0/0/0
```

http client ssl

To configure Secure Socket Layer (SSL) version to be used for HTTPS requests, use the **http client ssl** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client ssl *version*

Syntax Description

ssl *version*	Specify the SSL version to be used for HTTPS requests. Select one of the following versions: • **tls1.0** - Forces TLSv1.0 to be used for HTTPS requests. • **tls1.1** - Forces TLSv1.1 to be used for HTTPS requests. • **tls1.2** - Forces TLSv1.2 to be used for HTTPS requests. • **tls1.3** - Forces TLSv1.3 to be used for HTTPS requests. By default libcurl does not force the TLS version.

Command Default

By default, the SSL version is not configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 24.3.1	The support for SSL version TLS 1.3 was added.

Usage Guidelines

Use this command to configure the ssl version to be used in HTTPS requests.

Task ID

Task ID	Operations
config-servicess	read, write

The following example shows how to configure the SSL version to tls1.1:

```
RP/0/RP0/CPU0:router(config)#http client ssl tls1.1
```

http client tcp-window-scale

To configure the TCP window scale factor for high latency links, use the **http client tcp-window-scale** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client tcp-window-scale *scale*

Syntax Description

scale	Specify the TCP window scale for HTTP requests. Range is 1 to 14.

Command Default

By default, TCP window scale is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.3.6	This command was introduced.

Usage Guidelines

Use this command to configure the TCP window scale for HTTP requests.

Note Currently, this is enabled for copying of files using HTTP.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to set the TCP window scale to 10:

```
RP/0/RP0/CPU0:router(config)#http client tcp-window-scale 10
```

http client version

To configure the HTTP version to be used for HTTP requests, use the **http client version** command in XR Config mode. To restore the default value, use the **no** form of this command.

http client version *version*

Syntax Description

version*version*	Specify the HTTP version to be used for HTTP requests. Select one of the following versions: • **1.0** - Forces HTTP1.0 to be used for all HTTP requests. • **1.1** - Forces HTTP1.1 to be used for all HTTP requests. • **default** - libcurl picks up HTTP version automatically.

Command Default

By default, libcurl does not force the HTTP version.

Note HTTP Client uses libcurl version 7.30

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to configure the HTTP version to be used in HTTP requests.

Task ID

Task ID	Operations
config-services	read, write

The following example shows how to configure the HTTP version to 1.1:

```
Router(config)#http client version 1.1
```

http client vrf

To configure a new VRF to be used by the HTTP client, use the **http client vrf** command. To remove the specified vrf, use the **no** form of this command.

http **client** **vrf** *vrf-name*

Syntax Description

vrf-name	Specifies the name of the VRF to be used by the HTTP client.

Command Default

If not configured, the default VRF "default-vrf" will be used.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A HTTP client can have only one VRF. If a specific VRF is not configured for the HTTP client, the default VRF is assumed.

Task ID

Task ID	Operations
config-services	read, write

The following example shows the HTTP client being configured to start with the specified VRF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# http client vrf green
```

logging source-interface vrf

To configure the logging source interface in order to identify the syslog traffic that originates in a VRF from a particular router, as coming from a single device, use the **logging source-interface vrf** command in XR Config mode. To remove the source-interface logging configuration for the given VRF, use the **no** form of this command.

logging source-interface *interface* **vrf** *vrf-name*
no logging source-interface *interface* **vrf** *vrf-name*

Syntax Description

interface	Interface number of the source
vrf-name	Name that identifies the VRF

Command Default

If *vrf-name* is not specified, the source interface is configured for the default VRF.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to exit the router. The **logging source-interface** command configures the syslog packets to contain the IPv4 or IPv6 address of a particular interface for a VRF, regardless of which interface the packet uses to exit the router.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to configure interface loopback 0 to be the logging source interface for VRF vrf1.

```
Router#logging source-interface loopback 0 vrf vrf1
Router#logging source-interface loopback 1 vrf default
```

This sample output shows a logging source interface that is correctly configured for the VRF.

```
Router#show running-config logging
Wed Mar 4 07:37:48.974 UTC
logging console disable
logging source-interface Loopback0 vrf vrf1
```

ping bulk (network)

To check reachability and network connectivity to multiple hosts on IP networks, use the **ping bulk** command in XR EXEC mode.

ping bulk ipv4 [**input cli** [**batch** | **inline**]]
[**vrf** *vrf-name*] [**ip-address** | **domain-name**]

Syntax Description

ipv4	Specifies IPv4 address prefixes.
input	Specifies input mode.
cli	Specifies input via CLI.
batch	Pings after all destinations are input.
inline	Pings after each destination is input.
vrf *vrf-name ip-address domain-name*	(Optional) Specifies a particular VRF. IP address of the system to ping. (Optional) Domain name of the system to ping. **Note** You must hit the Enter button and then specify one destination address per line.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

You must hit the Enter button and then specify one destination address per line.

Maximum number of destinations you can specify in the cli or batch mode is 2000.

Task ID

Task ID	Operation
basic-services	read, write, execute

Example

The following example shows how to ping many hosts by the input via CLI method:

```
Router# ping bulk ipv4 input cli batch
```

```
Please enter input via CLI with one destination per line and when done Ctrl-D/(exit)
to initiate pings:
1: vrf myvrf1 10.2.1.16
2:
Starting pings...
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.16, vrf is myvrf1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms
```

```
Router# ping bulk ipv4 input cli

Please enter input via CLI with one destination per line:
vrf myvrf1 1.1.1.1
vrf myvrf2 2.2.2.2
vrf myvrf1 myvrf1.cisco.com
vrf myvrf2 myvrf2.cisco.com

Starting pings...
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/4/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/3/1 ms
```

ping (network)

To check host reachability and network connectivity on IP networks, use the **ping** command in XR EXEC mode.

ping [**ipv4** | **ipv6**] [*host-nameip-address*] [**count** *number*] [**size** *number*] [**source** {*ip-addressinterface-name* | **type** *number*}] [**timeout** *seconds*] [**pattern** *number*] [**type** *number*] [**priority** *number*][**verbose**] [**donnotfrag**] [**validate**] [**sweep**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
A.B.C.D	Target end address of the pseudowire.
host-name	(Optional) Hostname of the system to ping.
ip-address	(Optional) IP address of the system to ping.
count *number*	(Optional) Sets the repeat count. Range is 0 to 2147483647.
size *number*	(Optional) Sets the datagram size. Range is 36 to 18024
source	(Optional) Identifies the source address or source interface.
type *number*	(Optional) Sets the type of service. Range is 0 to 255. Available when the **ipv4** keyword is specified.
timeout *seconds*	(Optional) Sets the timeout in seconds. Range is 0 to 3600.
priority *number*	(Optional) Sets the packet priority. Range is 0 to 15. Available when the **ipv6** keyword is specified.
pattern *number*	(Optional) Sets the data pattern. Range is 0 to 65535.
verbose	(Optional) Sets verbose output.
donnotfrag	(Optional) Sets the Don’t Fragment (DF) bit in the IP header.
validate	(Optional) Validates the return packet.
sweep	(Optional) Sets the sweep ping.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The default value for the **ping** command refers only to the target IP address. No default value is available for the target IP address.

The ping program sends an echo request packet to an address and then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Note The **ping** (EXEC) command is supported only on IP networks.

If you enter the command without specifying either a hostname or an IP address, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter.

If the system cannot map an address for a hostname, it returns an "%Unrecognized host or address, or protocol not running" error message.

To abnormally terminate a ping session, enter the escape sequence, which is, by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

This table describes the test characters sent by the ping facility.

Table 27: ping Test Characters

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown packet type.
U	A "destination unreachable" error protocol data unit (PDU) was received.
C	A "congestion experienced" packet was received.
M	Fragmentation is needed, but the "don't fragment" bit in the IP header is set. When this bit is set, the IP layer does not fragment the packet and returns an Internet Control Message Protocol (ICMP) error message to the source if the packet size is larger than the maximum transmission size. When this bit is not set, the IP layer fragments the packet to forward it to the next hop.
Q	A source quench packet was received.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

Although the precise dialog varies somewhat between IPv4 and IPv6, all are similar to the ping session, using default values shown in the following output:

```
Router# ping

Protocol [ipv4]:
Target IP address: 10.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```
Extended commands? [no]: yes
Source address or interface: 10.0.0.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]: yes
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.58.21, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/49 ms
```

If you enter a hostname or an address on the same line as the **ping** command, the command performs the default actions appropriate for the protocol type of that hostname or address, as shown in the following output:

```
Router# ping server01

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
```

scp

To securely transfer a file from a local directory to a remote directory or from a remote directory to a local directory, use the **scp** command in XR EXEC mode.

scp {*local-directory username@location/directory*} / *filename* {*username@location/directory local-directory* } / *filename*

Syntax Description

local-directory	Specifies the local directory on the device.
username@location/directory	Specifies the remote directory where *location* is the IP address of the remote device.
filename	Specifies the file name to be transferred.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Secure Copy Protocol (SCP) is a file transfer protocol which provides a secure and authenticated method for transferring files. SCP relies on SSHv2 to transfer files from a remote location to a local location or from local location to a remote location.

Use the **scp** command to copy a file from the local device to a destination device or from a destination device to the local device.

Using SCP, you can only transfer individual files. You cannot transfer a file from a remote device to another remote device.

SSH server process must be running on the remote device.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to copy a file using the **scp** command from a local directory to a remote directory:

```
Router# scp /usr/file1.txt root@209.165.200.1:/root/file3.txt

Connecting to 209.165.200.1...
Password:
  Transferred 553065 Bytes
  553065 bytes copied in 0 sec (7576232)bytes/sec
```

The following example shows how to copy a file using the **scp** command from a remote directory to a local directory:

```
Router# scp root@209.165.200.1:/root/file4.txt /usr/file.txt

Connecting to 209.165.200.1...
Password:
  Transferred 553065 Bytes
  553065 bytes copied in 0 sec (7576232)bytes/sec
```

show cinetd services

To display the services whose processes are spawned by Cinetd when a request is received, use the **show cinetd services** command in XR Exec mode.

show cinetd services

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample is output from the **show cinetd services** command:

```
RP/0/RP0/CPU0:router# show cinetd services

Vrf Name          Family Service Proto Port ACL max_cnt curr_cnt wait Program Client Option

context-management v4    tftp   udp   69      unlimited       0    wait ttfpd sysdb  disk0:
default            v4    telnet   tcp   23       100       2    nowait telnetd sysdb  disk0
```

This table describes the significant fields shown in the display.

Table 28: show cinetd services Command Field Descriptions

Field	Description
Family	Version of the network layer (IPv4 or IPv6).
Service	Network service (for example, FTP, Telnet, and so on).
Proto	Transport protocol used by the service (tcp or udp).
Port	Port number used by the service.
ACL	Access list used to limit the service from some hosts.
max_cnt	Maximum number of concurrent servers allowed for a service.

Field	Description
curr_cnt	Current number of concurrent servers for a service.
wait	Status of whether Cinetd has to wait for a service to finish before serving the next request.
Program	Name of the program for a service.
Option	Service-specific options.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses, use the **show hosts** command in XR EXEC mode.

show hosts [*host-name*]

Syntax Description

host-name	(Optional) Name of the host about which to display information. If omitted, all entries in the local cache are displayed.

Command Default

Unicast address prefixes are the default when IPv4 address prefixes are configured.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show hosts** command:

```
Router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host              Flags        Age(hr)   Type       Address(es)
host1.cisco.com    (temp, OK)    1         IP         192.168.4.10
abc              (perm, OK)    0         IP         10.0.0.0 10.0.0.2 10.0.0.3
```

This table describes the significant fields shown in the display.

Table 29: show hosts Command Field Descriptions

Field	Description
Default domain	Default domain used to complete the unqualified hostnames.
Name/address lookup	Lookup is disabled or uses domain services.
Name servers	List of configured name servers.
Host	Hostname.

Field	Description
Flags	Indicates the status of an entry. • temp—Temporary entry entered by a name server; the software removes the entry after 72 hours of inactivity. • perm—Permanent entry entered by a configuration command; does not time out. • OK—Entry is believed to be valid. • ??—Entry is considered suspect and subject to revalidation. • EX—Entry has expired.
Age(hr)	Number of hours since the software most recently referred to the cache entry.
Type	Type of address (IPv4 or IPv6).
Address(es)	Address of the host. One host may have up to eight addresses.

telnet

To log in to a host that supports Telnet, use the **telnet** command in XR EXEC mode.

telnet [**vrf** {*vrf-name* | **default**}] {*ip-address* | *host-name*} [*options*]

Syntax Description

vrf	(Optional) Specifies a VPN routing and forwarding (VRF) instance
vrf-name	VRF name of the system to ping.
default	Specifies the default VRF instance.
ip-address	IP address of a specific host on a network. • IPv4 address format—Must be entered in the (*x.x.x.x*) format. • IPv6 address format— Must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host-name	Name of a specific host on a network.
options	(Optional) Telnet connection options. See **Telnet Connection Options** for a list of supported options.

Command Default

Telnet client is in Telnet connection options nostream mode.

Command Modes

XR EXEC mode

Command History

Release	**Modification**
Release 7.0.12	This command was introduced.

Usage Guidelines

If the Telnet server is enabled, you should be able to start a Telnet session as long as you have a valid username and password.

This table lists the supported Telnet connection options.

Table 30: Telnet Connection Options

Option	Description
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX copy program (UUCP) and other non-Telnet protocols.
/nostream	Turns off stream processing.
port number	Port number. Range is 0 to 65535.
/source-interface	Specifies source interface.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Control and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. **Special Telnet Escape Sequences** lists the special Telnet escape sequences.

Table 31: Special Telnet Escape Sequences

Escape Sequence[7]	Purpose
Ctrl-^ c	Interrupt Process (IP).
Ctrl-^ o	Terminates Output (AO).
Ctrl-^ u	Erase Line (EL).

[7] The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

ctrl-^?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Control key, and the second caret represents Shift-6 on your keyboard:

```
Router# ^^?
```

```
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 and then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, issue any of the following commands at the prompt of the device to which you are connecting:

- close
- disconnect
- exit
- logout
- quit

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

The following example shows how to establish a Telnet session to a remote host named host1:

```
Router# telnet host1
```

telnet client source-interface

To specify the source IP address for a Telnet connection, use the **telnet client source-interface** command in XR Config mode. To remove the **telnet client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

telnet {**ipv4** | **ipv6**} **client** **source-interface** *type* *interface-path-id*
no **telnet** **client** **source-interface** *type* *interface-path-id*

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The IP address of the best route to the destination is used as the source IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **telnet client source-interface** command to set the IP address of an interface as the source for all Telnet connections.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to set the IP address for HundredGigE interface 1/0/2/1 as the source address for Telnet connections:

```
Router(config)# telnet ipv4 client source-interface hundredgige1/0/2/1
```

telnet dscp

To define the differentiated services code point (DSCP) value and IPv4 precedence to specifically set the quality-of-service (QoS) marking for Telnet traffic on a networking device, use the **telnet dscp** command in XR Config mode. To disable DSCP, use the **no** form of this command.

telnet [**vrf** {*vrf-name* | **default**}] **ipv4** **dscp** *dscp-value*
no **telnet** [**vrf** {*vrf-name* | **default**}] **ipv4** **dscp** *dscp-value*

Syntax Description

vrf	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
default	(Optional) Specifies the default VRF instance.
ipv4	Specifies IPv4 address prefixes.
dscp-value	Value for DSCP. The range is from 0 to 63. The default value is 0.

Command Default

If DSCP is disabled or not configured, the following default values are listed:

- The default value for the server 16.
- The default value for the client is 0.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

IPv4 is the supported protocol for defining a DSCP value for locally originated Telnet traffic.

DSCP can impact both server and client behavior of the specific VRF.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to define the DSCP value and IPv4 precedence:

```
Router(config)# telnet vrf default ipv4 dscp 40
Router(config)# telnet vrf default ipv4 dscp 10
```

telnet server

To enable Telnet services on a networking device, use the **telnet server** command in XR Config mode. To disable Telnet services, use the **no** form of this command.

telnet [**vrf** {*vrf-name* | **default**}] {**ipv4** | **ipv6**} **server max-servers** {**no-limit***limit*} [**access-list** *list-name*]
no telnet [**vrf** {*vrf-name* | **default**}] {**ipv4** | **ipv6**} **server max-servers** {**no-limit***limit*} [**access-list** *list-name*]

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
default	(Optional) Specifies the default VRF instance.
ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
max-servers	Sets the number of allowable Telnet servers.
no-limit	Specifies that there is no maximum number of allowable Telnet servers.
limit	Specifies the maximum number of allowable Telnet servers. Range is 1 to 200.
access-list	(Optional) Specifies an access list.
list-name	(Optional) Access list name.

Command Default

Telnet services are disabled.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Disable Telnet services to prevent inbound Telnet connections from being accepted into a networking device using the **telnet** command. After Telnet services are disabled, no new inbound connections are accepted, and the Cisco Internet services daemon (Cinetd) stops listening on the Telnet port.

Enable Telnet services by setting the **max-servers** keyword to a value of one or greater. This allows inbound Telnet connections into a networking device.

This command affects only inbound Telnet connections to a networking device. Outgoing Telnet connections can be made regardless of whether Telnet services are enabled.

Using the **no** form of the command disables the Telnet connection and restores the system to its default condition.

Note Before establishing communications with the router through a Telnet session, configure the telnet server and vty-pool functions (see *System Management Command Reference for Cisco 8000 Series Routers*, *System Management Configuration Guide for Cisco 8000 Series Routers*, and *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to enable Telnet services for one server:

```
Router(config)# telnet ipv4 server max-servers 1
```

telnet transparent

To send a Carriage Return (CR) as a CR-NULL rather than a Carriage Return-Line Feed (CR-LF) for virtual terminal sessions, use the **telnet transparent** command in line template submode. To remove the **telnet transparent** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

telnet transparent
no telnet transparent

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Line console

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **telnet transparent** command is useful for coping with different interpretations of end-of-line handling in the Telnet protocol specification.

Task ID

Task ID	Operations
tty-access	read, write

Examples

The following example shows how to configure the vty line to operate in Telnet transparent mode so that when the carriage return key is pressed the system sends the signal as a CR-NULL key combination rather than a CR-LF key combination:

```
Router(config)# line console
Router(config-line)# telnet transparent
```

tftp server

To enable or disable the TFTP server or a feature running on the TFTP server, use the **tftp server** command in XR Config mode.

tftp { **ipv4** | **ipv6** } **server** **homedir** *tftp-home-directory* [**max-servers** [*number* | **no-limit**] | **access-list** *name*]

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
homedir *tftp-home-directory*	Specifies the home directory.
max-servers *number*	(Optional) Sets the maximum number of concurrent TFTP servers. The range is from 1 to 2147483647.
max-servers no-limit	(Optional) Sets no limit to process a number of allowable TFTP server.
access-list *name*	(Optional) Specifies the name of the access list associated with the TFTP server.

Command Default

The TFTP server is disabled by default. When not specified, the default value for the **max-servers** keyword is unlimited.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

Using the **no** form of the **tftp server** command removes the specified command from the configuration file and restores the system to its default condition. The **no** form of the command is not stored in the configuration file.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows that the TFTP server is enabled for the access list named test:

```
RP/0/RP0/CPU0:router(config)# tftp ipv4 server homedir disk0 access-list test
```

tftp client source-interface

To specify the source IP address for a TFTP connection, use the **tftp client source-interface** command in XR Config mode. To remove the **tftp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

tftp client source-interface *type interface-path-id*
no tftp client source-interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

The IP address of the best route to the destination is used as the source IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **tftp client source-interface** command to set the IP address of an interface as the source for all TFTP connections.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the IP address for HundredGigE interface 1/0/2/1 as the source address for TFTP connections:

```
Router(config)# tftp client source-interface hundredgige1/0/2/1
```

traceroute

To discover the routes that packets actually take when traveling to their destination across an IP network, use the **traceroute** command in XR EXEC mode.

traceroute [**ipv4** | **ipv6**] [*host-nameip-address*] [{**source***ip-address-nameinterface-name*}] [**numeric**] [**timeout** *seconds*] [**probe** *count*] [**minttl** *seconds*] [**maxttl** *seconds*] [**port** *number*] [**priority** *number*] [**verbose**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
host-name	(Optional) Hostname of system to use as the destination of the trace attempt.
ip-address	(Optional) Address of system to use as the destination of the trace attempt.
source	(Optional) Source address.
ip-address-name	(Optional) IP address A.B.C.D or hostname.
numeric	(Optional) Numeric display only.
timeout *seconds*	(Optional) Timeout value. Range is 0 to 3600.
probe *count*	(Optional) Probe count. Range is 0 to 65535.
minttl *seconds*	(Optional) Minimum time to live. Range is 0 to 255.
maxttl *seconds*	(Optional) Maximum time to live. Range is 0 to 255.
port *number*	(Optional) Port number. Range is 0 to 65535.
priority *number*	(Optional) Packet priority. Range is 0 to 15. Available when the **ipv6** keyword is specified.
verbose	(Optional) Verbose output.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The default value for the **traceroute** command refers only to the destination. No default value is available for the destination address.

The **traceroute** command works by taking advantage of the error messages generated by networking devices when a datagram exceeds its time-to-live (TTL) value.

The **traceroute** command starts by sending probe datagrams with a TTL value of 1, which causes the first networking device to discard the probe datagram and send back an error message. The **traceroute** command sends several probes at each TTL level and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time-exceeded” error message indicates that an intermediate networking device has seen and discarded the probe. A “destination-unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence, which is, by default, Ctrl-C. Simultaneously press and release the Ctrl and C keys.

To use nondefault parameters and invoke an extended **traceroute** test, enter the command without a *host-name* or *ip- address* argument. You are stepped through a dialog to select the desired parameter values for the **traceroute** test.

Because of how IP is implemented on various networking devices, the IP **traceroute** command may behave in unexpected ways.

Not all destinations respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message, but they reuse the TTL of the incoming packet. Because this value is zero, the ICMP packets do not succeed in returning. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL is raised high enough that the “ICMP” message can get back. For example, if the host is six hops away, the **traceroute** command times out on responses 6 through 11.

Task ID

Task ID	Operations
basic-services	read, write, execute

Examples

The following output shows a sample **traceroute** session when a destination hostname has been specified:

```
Router# traceroute host8-sun

Type escape sequence to abort.
Tracing the route to 192.168.0.73
 1 192.168.1.6 (192.168.1.6) 10 msec 0 msec 10 msec
 2 gateway01-gw.gateway.cisco.com (192.168.16.2) 0 msec 10 msec 0 msec
 3 host8-sun.cisco.com (192.168.0.73) 10 msec * 0 msec
```

The following display shows a sample extended **traceroute** session when a destination hostname is not specified:

```
traceroute# traceroute

Protocol [ipv4]:
Target IP address: ena-view3
Source address: 10.0.58.29
Numeric display? [no]:
Timeout in seconds [3]:
```

```
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:

Type escape sequence to abort.
Tracing the route to 171.71.164.199
 1  sjc-jpxlnock-vpn.cisco.com (10.25.0.1) 30 msec  4 msec  4 msec
 2  15lab-vlan725-gx1.cisco.com (173.19.72.2) 7 msec  5 msec  5 msec
 3  stc15-00lab-gw1.cisco.com (173.24.114.33) 5 msec  6 msec  6 msec
 4  stc5-lab4-gw1.cisco.com (173.24.114.89) 5 msec  5 msec  5 msec
 5  stc5-sbb4-gw1.cisco.com (172.71.241.162) 5 msec  6 msec  6 msec
 6  stc5-dc5-gw1.cisco.com (172.71.241.10) 6 msec  6 msec  5 msec
 7  stc5-dc1-gw1.cisco.com (172.71.243.2) 7 msec  8 msec  8 msec
 8  ena-view3.cisco.com (172.71.164.199) 6 msec  *  8 msec
```

This table describes the characters that can appear in traceroute output.

Table 32: traceroute Text Characters

Character	Description
xx msec	For each node, the round-trip time in milliseconds for the specified number of probes.
*	Probe time out.
?	Unknown packet type.
A	Administratively unreachable. This output usually indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

LPTS Commands

This chapter describes the Cisco IOS XR software commands used to monitor Local Packet Transport Services.

For detailed information about LPTS concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

clear lpts ifib statistics

To clear the Internal Forwarding Information Base (IFIB) statistics, use the **clear lpts ifib statistics** command in XR EXEC mode.

clear lpts ifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	Clears the IFIB statistics for the designated node. The *node-id* argument is entered in standard *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	execute

Examples

The following example shows how to clear the IFIB statistics for the RP:

```
RP/0/RP0/CPU0:router# clear lpts ifib statistics
```

clear lpts pifib statistics

To clear the Pre-Internal Forwarding Information Base (Pre-IFIB) statistics, use the **clear lpts pifib statistics** command in XR EXEC mode.

clear lpts pifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	Clears the Pre-IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	execute

Examples

The following example shows how to clear the Pre-IFIB statistics for the RP:

```
RP/0/RP0/CPU0:router# clear lpts pifib statistics location 0/RP0/CPU0
```

flow (LPTS)

To configure the policer for the Local Packet Transport Services (LPTS) flow type, use the **flow** command in pifib policer global configuration mode or pifib policer per-node configuration mode. To disable this feature, use the **no** form of this command.

flow *flow-type* **rate** *rate*
no flow *flow-type* **rate** *rate*

Syntax Description

flow-type	List of supported flow types.
rate *rate*	Specifies the rate in packets per seconds (PPS). The range is from 0 to 50000.

Command Default

The default behavior is to load the policer values from the static configuration file that is platform dependant.

Command Modes

Pifib policer global configuration

Pifib policer per-node configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The table lists the supported flow types and the parameters that are used to define a policer.

Table 33: List of Supported Flow Types

Flow Type	Description	Default Packet Rate (Recommended)	
BGP-default	SRC port 179 and Dest Port 179 with protocol as TCP.	4000	
fragment	IPv4/v6 fragmented packets.	1000	
ICMP-default	All ICMP type packets.	2500	
ISIS default	All ISIS protocol packets.	3500	

Flow Type	Description	Default Packet Rate (Recommended)	
LDP-UDP	UDP with Destination Port 646.	2000	
OSPF-MC-default	OSPFv2 (224.0.0.5, 224.0.0.6), OSPFv3 (FF02::5 and FF02::6).	3500	
OSPF-UC-default	OSPFv2 and OSPFv3 Unicast DBD packets.	3000	
RAW-default	RAW default entry in LPTS.	500	
RSVP-default	All RSVP protocol packets (RSVP signalling, refresh etc...).	14500	
TCP-default	All TCP protocol packets (TCP-known, cfg-peer, listen).	25500	
Third party applications	All third party application packets.	10000	
UDP-default	All UDP protocol packets (UDP-known, CFG-peer, listen).	25500	

Task ID

Task ID	Operations
config-services	read, write

Examples

The following example shows how to configure the LPTS policer for the bgp-default flow type for all line cards:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# lpts pifib hardware police
RP/0/RP0/CPU0:router(config-pifib-policer-global)# flow bgp-default rate 4000
```

The following example shows how to configure LPTS policer for the Intermediate System-to-Intermediate System (IS-IS)-default flow type for a specific line card:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:routerconfig)# lpts pifib hardware police location 0/2/CPU0
RP/0/RP0/CPU0:router(config-pifib-policer-per-node)# flow isis-default rate 22222
```

lpts pifib hardware dynamic-flows

To configure LPTS flow types and define the maximum LPTS entries for each flow type in the TCAM use the **lpts pifib hardware dynamic-flows** in configuration mode.

lpts pifib hardware dynamic-flows location *node-id* **flow** *flow-type* **max** *maximum-flow-entries*

Syntax Description

location*node-id*	Configures Dynamic LPTS per node. The *node-id* argument is entered inthe rack/slot/module notation. For more information, use the question mark (?) online help function
flow *flow-type*	Configures speficied flow type.
max *maximum-flow-entries*	Configures maximum flow entries per node. **Note** The maximum flow entry value of zero denotes that a flow type is not configured. For more information, use the question mark (?) online help function

Command Default

Dynamic LPTS is disabled

Command Modes

Configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The sum of maximum LPTS entries configured for all flow types must not exceed 16000 entries. User can configure only configurable LPTS flow types listed in below table.

Table 34: Configurable Flow Types and Default Maximum Flow Entries

Flow Type	Default Maximum Flow Entries
BGP-known	900
BGP-cfg-peer	900
IP-SLA	50
LDP-TCP-known	300
LDP-TCP-cfg-peer	300
SSH-known	150
Telnet Known	150

Flow Type	Default Maximum Flow Entries
NTP known	150
LDP-UDP	300
OSPF-uc-known	300
OSPF-mc-known	600
RSVP known	300
ISIS known	300
TPA	5
PIM-mcast-known	300
IGMP	1200
SNMP	300
VRRP	150
DNS	40
All-routers	300

Note You can increase or decrease the flow entries of any flow type in such a way that the total of flow entries add up to 8000.

Task ID

Task ID	Operation
lpts	read, write
config-services	read, write

In this example you will configure the BGP-known and ISIS-known LPTS flow type in the TCAM and define the maximum flow entries as 1800 and 500 for node location 0/1/CPU0.

```
Router#configure
Router(config)#lpts pifib hardware dynamic-flows location 0/1/CPU0
Router(config-pifib-flows-per-node)#flow bgp-known max 1800
Router(config-pifib-flows-per-node)#flow ISIS-known max 500
```

lpts pifib hardware police

To configure the ingress policers and to enter pifib policer global configuration mode or pifib policer per-node configuration mode, use the **lpts pifib hardware police** command in XR Config mode. To set the policer to the default value, use the **no** form of this command.

lpts pifib hardware police [**location** *node-id*] [**flow** *flow-type* { **default** } [**rate** *rate*]
no lpts pifib hardware police [**location** *node-id*] [**flow** *flow-type* { **default** } [**rate** *rate*]

Syntax Description

location *node-id*	(Optional) Designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
flow *flow-type* **rate** *rate*	LPTS flow type and the policer rate in packets per second (PPS).
default	Indicates generic flows which are policed with default-rate. For example, BGP (*, 179), any packet with port:179 policed with default rate.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

- Provided that the apllication and the IP-SLA processing rates support it, you can specify the flow rate for IP-SLA flow entries to up to 1500.
- When configuring the HSRP IPv6 networks on Physical interfaces, Physical sub-interfaces, Bundle interfaces, and Bundle sub-interfaces on the Cisco Silicon One P100 and Cisco Silicon One Q200 ASIC-based systems, for a scale higher than the supported scale of IPv6 HSRP groups, set the default UDP entry policy rate to 3000 or higher to avoid any LPTS drops. For information about the supported scale, see HSRP over Physical Interfaces and Bundle Interfaces.
- When configuring the HSRP/VRRP IPv4 or IPv6 networks on Physical interfaces, Physical sub-interfaces, Bundle interfaces, and Bundle sub-interfaces on the Cisco Silicon One P100 and Cisco Silicon One Q200 ASIC-based systems, for HSRP/VRRP IPv4 or IPv6 groups with a scale higher than the supported scale or groups with aggressive timer values less than 1 second, increase the LPTS policer rate to 3000 or higher to avoid any LPTS drops. For information about the supported scale, see:
  - HSRP over Physical Interfaces and Bundle Interfaces
  - VRRP over Physical Interfaces and Bundle Interfaces

Task ID

Task ID	Operations
lpts	read, write
config-services	read, write

Examples

This example shows how to configure the **lpts pifib hardware police** command for all line cards:

```
RP/0/RP0/CPU0:router(config)# lpts pifib hardware police
RP/0/RP0/CPU0:router(config-pifib-policer-global)#
```

This example shows how to configure the **lpts pifib hardware police** command for a specific line card:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# lpts pifib hardware police location 0/2/CPU0
```

This example shows how to set the default UDP entry policer rate in the **lpts pifib hardware police** command for a specific line card:

```
RP/0/RP0/CPU0:ios(config)#lpts pifib hardware police location 0/0/CPU0 flow udp default
rate 1000
RP/0/RP0/CPU0:ios(config)#commit
Mon Apr 22 22:42:15.322 UTC
RP/0/RP0/CPU0:ios(config)#
```

This example sets the default UDP entry policer rate to 3000 so that there will not be any LPTS drops for HSRP flows for a higher scale.

```
RP/0/RP0/CPU0:ios(config)#lpts pifib hardware police location 0/0/CPU0 flow udp default
rate 3000
RP/0/RP0/CPU0:ios(config)#commit
```

These examples set the LPTS policer rate to 3000 for HSRP and VRRP so that there will not be any LPTS drops for HSRP/VRRP flows for a higher scale.

```
RP/0/RP0/CPU0:ios#configure
Tue Apr 23 05:06:31.016 UTC
RP/0/RP0/CPU0:ios(config)#lpts pifib hardware police
RP/0/RP0/CPU0:ios(config-lpts-policer-global)#flow hsrp rate 3000
RP/0/RP0/CPU0:ios(config-lpts-policer-global)#commit
Tue Apr 23 05:07:13.440 UTC
```

```
RP/0/RP0/CPU0:ios#configure
Tue Apr 23 05:06:31.016 UTC
RP/0/RP0/CPU0:ios(config)#lpts pifib hardware police
RP/0/RP0/CPU0:ios(config-lpts-policer-global)#flow vrrp rate 3000
RP/0/RP0/CPU0:ios(config-lpts-policer-global)#commit
Tue Apr 23 05:07:13.440 UTC
```

show lpts bindings

To display the binding information in the Port Arbitrator, use the **show lpts bindings** command in XR EXEC mode.

show lpts bindings [**location** *node-id*] [**client-id** {**clnl** | **ipsec** | **ipv4-io** | **ipv6-io** | **mpa** | **tcp** | **test** | **udp** | **raw**}] [**brief**] [**vrf** *vrf-name*]

Syntax Description

location *node-id*	(Optional) Displays information for the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.
client-id	(Optional) Type of client. It can be one of the following values: • **clnl** —ISO connectionless protocol (used by IS-IS) • **ipsec** —Secure IP • **ipv4-io** —Traffic processed by the IPv4 stack • **ipv6-io** —Traffic processed by the IPv6 stack • **mpa** —Multicast Port Arbitrator (multicast group joins) • **tcp** —Transmission Control Protocol • **test** —Test applications • **udp** —User Datagram Protocol • **raw** —Raw IP
brief	(Optional) Displays summary output.
vrf *vrf-name*	(Optional) Name of assigned VRF.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show lpts bindings** command displays the Local Packet Transport Services (LPTS) bindings (requests to receive traffic of a particular type). Bindings are aggregated into flows by the LPTS Port Arbitrator; flows are then programmed into the Internal Forwarding Information Base (IFIB) and Pre-IFIB to direct packets to applications.

If you specify the optional **client-id** keyword and type of client, only bindings from that client are shown. If you specify the optional **location** keyword and *node-id* argument, only bindings from clients on that node are displayed.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts bindings** command, displaying bindings for all client ID types:

```
RP/0/RP0/CPU0:router# show lpts bindings

@ - Indirect binding; Sc - Scope

------------------------------------------
Location   :0/1/CPU0
Client ID  :IPV4_IO
Cookie     :0x00000001
Clnt Flags :
Layer 3    :IPV4
Layer 4    :ICMP
Local Addr :any
Remote Addr:any
Local Port :any
Remote Port:any
Filters    :Type / Intf or Pkt Type / Source Addr / Location
 INCLUDE_TYPE / type 8
 INCLUDE_TYPE / type 13
 INCLUDE_TYPE / type 17
------------------------------------------
Location   :0/2/CPU0
Client ID  :IPV4_IO
Cookie     :0x00000001
Clnt Flags :
Layer 3    :IPV4
Layer 4    :ICMP
Local Addr :any
Remote Addr:any
Local Port :any
Remote Port:any
Filters    :Type / Intf or Pkt Type / Source Addr / Location
 INCLUDE_TYPE / type 8
 INCLUDE_TYPE / type 13
 INCLUDE_TYPE / type 17
------------------------------------------
Location   :0/RP1/CPU0
Client ID  :TCP
Cookie     :0x4826f1f8
Clnt Flags :REUSEPORT
Layer 3    :IPV4
Layer 4    :TCP
Local Addr :any
Remote Addr:any
Local Port :7
Remote Port:any
------------------------------------------
Location   :0/RP1/CPU0
Client ID  :TCP
Cookie     :0x4826fa0c
Clnt Flags :REUSEPORT
Layer 3    :IPV4
Layer 4    :TCP
```

```
Local Addr :any
Remote Addr:any
Local Port :9
Remote Port:any
------------------------------------------
Location   :0/RP1/CPU0
Client ID  :TCP
Cookie     :0x482700d0
Clnt Flags :REUSEPORT
Layer 3    :IPV4
Layer 4    :TCP
Local Addr :any
Remote Addr:any
Local Port :19
Remote Port:any
------------------------------------------
Location   :0/RP1/CPU0
Client ID  :IPV4_IO
Cookie     :0x00000001
Clnt Flags :
Layer 3    :IPV4
Layer 4    :ICMP
Local Addr :any
Remote Addr:any
Local Port :any
Remote Port:any
Filters    :Type / Intf or Pkt Type / Source Addr / Location
 INCLUDE_TYPE / type 8
 INCLUDE_TYPE / type 13
 INCLUDE_TYPE / type 17
```

This table describes the significant fields shown in the display.

Table 35: show lpts bindings Command Field Descriptions

Field	Description
Location	Node location, in the format of *rack/slot/module*.
Client ID	LPTS client type.
Cookie	Client’s unique tag for the binding.
Clnt Flags	REUSEPORT -- client has set the SO_REUSEPORT or SO_REUSEADDR socket option.
Layer 3	Layer 3 protocol (IPv4, IPv6, CLNL).
Layer 4	Layer 4 protocol (TCP, UDP).
Local Addr	Local (destination) address.
Remote Addr	Remote (source) address.
Local Port	Local (destination) TCP or UDP port, or ICMP/IGMP packet type, or IPsec SPI.
Remote Port	Remote (source) TCP or UDP port.

The following sample output is from the **show lpts bindings brief** command:

```
RP/0/RP0/CPU0:router# show lpts bindings brief

@ - Indirect binding; Sc - Scope

 Location   Clnt Sc L3   L4    VRF-ID   Local,Remote Address.Port  Interface
 ---------- ---- -- ---- ----- -------- -------------------------- ------------
 0/1/CPU0   IPV4 LO IPV4 ICMP  *        any.ECHO any               any
 0/1/CPU0   IPV4 LO IPV4 ICMP  *        any.TSTAMP any             any
 0/1/CPU0   IPV4 LO IPV4 ICMP  *        any.MASKREQ any            any
 0/1/CPU0   IPV6 LO IPV6 ICMP6 *        any.ECHOREQ any            any
 0/3/CPU0   IPV4 LO IPV4 ICMP  *        any.ECHO any               any
 0/3/CPU0   IPV4 LO IPV4 ICMP  *        any.TSTAMP any             any
```

This table describes the significant fields shown in the display.

Table 36: show lpts bindings brief Command Field Descriptions

Field	Description
Location	Node location, in the format of *rack/slot/module*.
Clnt ID	LPTS client type.
Sc	Scope (LR = Logical-Router, LO = Local).
Layer 3	Layer 3 protocol.
Layer 4	Layer 4 protocol.
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local,Remote Address.Port	Local (destination) and Remote (source) addresses and ports or packet types.
Interface	Inbound interface.

show lpts clients

To display the client information for the Port Arbitrator, use the **show lpts clients** command in XR EXEC mode.

show lpts clients [**times**]

Syntax Description

times	(Optional) Displays information about binding request rates and service times.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show lpts clients** command displays the clients connected to the local packet transport services (LPTS) port arbitrator (PA).

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts clients** command:

```
RP/0/RP0/CPU0:router# show lpts clients

o_flgs - open flags ; clid - client id
clid            loc             flags   o_flgs
RAW(3)          0/RP1/CPU0      0x1     0x2
TCP(1)          0/RP1/CPU0      0x1     0x2
IPV4_IO(5)      0/1/CPU0        0x3     0x2
IPV4_IO(5)      0/2/CPU0        0x3     0x2
IPV4_IO(5)      0/RP1/CPU0      0x3     0x2
MPA(7)          0/RP1/CPU0      0x3     0x0
```

This table describes the significant fields shown in the display.

Table 37: show lpts clients Command Field Descriptions

Field	Description
Clid	LPTS client ID.
Loc	Node location, in the format *rack/slot/module*.

Field	Description
Flags	Client flags. **Note** The client flags are used only for debugging purposes.
o_flags	Open flags. **Note** The open flags are used only for debugging purposes.

The following sample output is from the **show lpts clients times** command. The output shows samples for the last 30 seconds, 1 minute, 5 minutes, 10 minutes, and a total (if nonzero). The number of transactions, number of updates, and the minimum/average/maximum time in milliseconds to process each transaction is shown.

```
RP/0/RP0/CPU0:router# show lpts clients times

o_flgs - open flags ; clid - client id
clid            loc     flags   o_flgs
RAW(3)          0/RP1/CPU0      0x1     0x2
   30s:2 tx 2 upd 2/2/3ms/tx
    1m:2 tx 2 upd 2/2/3ms/tx
    5m:2 tx 2 upd 2/2/3ms/tx
   10m:2 tx 2 upd 2/2/3ms/tx
 total:2 tx 2 upd 2/-/3ms/tx
TCP(1)          0/RP1/CPU0      0x1     0x2
 total:3 tx 3 upd 1/-/1ms/tx
IPV4_IO(5)      0/1/CPU0        0x3     0x2
 total:1 tx 1 upd 0/-/0ms/tx
IPV4_IO(5)      0/2/CPU0        0x3     0x2
 total:1 tx 1 upd 1/-/1ms/tx
IPV4_IO(5)      0/RP1/CPU0      0x3     0x2
 total:1 tx 1 upd 3/-/3ms/tx
MPA(7)          0/RP1/CPU0      0x3     0x0
```

show lpts flows

To display information about Local Packet Transport Services (LPTS) flows, use the **show lpts flows** command in XR EXEC mode.

show lpts flows [**brief**]

Syntax Description

brief	(Optional) Displays summary output.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show lpts flows** command is used to display LPTS flows, which are aggregations of identical binding requests from multiple clients and are used to program the LPTS Internal Forwarding Information Base (IFIB) and Pre-IFIB.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts flows** command:

```
RP/0/RP0/CPU0:router# show lpts flows

------------------------------------------
L3-proto    : IPV4(2)
L4-proto    : ICMP(1)
VRF-ID      : * (000000000)
Local-IP    : any
Remote-IP   : any
Pkt-Type    : 8
Remote-Port : any
Interface   : any (0x0)
Flow-type   : ICMP-local
Min-TTL     : 0
Slice       : RAWIP4_FM
Flags       : 0x20 (in Pre-IFIB)
Location    : (drop)
Element References
location / count / scope
* / 3 / LOCAL
```

This table describes the significant fields shown in the display.

Table 38: show lpts flows Command Field Descriptions

Field	Description
L3-proto	Layer 3 protocol (IPv4, IPv6, CLNL).
L4-proto	Layer 4 protocol (TCP, UDP, and so on).
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local-IP	Local (destination) IP address.
Remote-IP	Remote (source) IP address.
Pkt-Type	ICMP or IGMP packet type.
Remote-Port	Remote (source) TCP or UDP port.
Interface	Ingress interface.
Flow-type	Flow classification for hardware packet policing.
Min-TTL	Minimum time-to-live value expected from in the incoming packet. Any packet received with a lower TTL value will be dropped.
Slice	IFIB slice.
Flags	• Has FGID: Delivered to multiple destinations. • No IFIB entry: IFIB entry suppressed. • Retrying FGID allocation. • In Pre-IFIB: Entry is in Pre-IFIB as well. • Deliver to one: If multiple bindings, will deliver to only one.
Location	*rack/slot/module* to deliver to.
Element References	• location: *rack/slot/module* of client. • count: number of clients at that location. • scope: binding scope (LR:Logical Router, LOCAL:Local).

The following sample output is from the **show lpts flows brief** command:

```
RP/0/RP0/CPU0:router# show lpts flows brief

+ - Additional delivery destination; L - Local interest; P - In Pre-IFIB

 L3   L4    VRF-ID   Local, Remote Address.Port      Interface    Location    LP
 ---- ----- -------- ------------------------------- ------------ ----------- --
 IPV4 ICMP  *        any.ECHO any                    any          (drop)      LP
 IPV4 ICMP  *        any.TSTAMP any                  any          (drop)      LP
 IPV4 ICMP  *        any.MASKREQ any                 any          (drop)      LP
 IPV6 ICMP6 *        any.ECHOREQ any                 any          (drop)      LP
 IPV4 any   default  224.0.0.2 any                   Gi0/1/0/1    0/5/CPU0     P
```

This table describes the significant fields shown in the display.

Table 39: show lpts flows brief Command Field Descriptions

Field	Description
L3	Layer 3 protocol (IPv4, IPv6, CLNL).
L4	Layer 4 protocol.
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local, Remote Address.Port	Local (destination) and remote (source) IP addresses and TCP or UDP ports, or ICMP/IGMP packet types, or IPSec Security Parameters Indices.
Interface	Ingress interface.
Location	Delivery location: • *rack/slot/module*—Individual location. • [0xNNNNN]—Multiple locations (platform-dependent value). • (drop)—Do not deliver to any application.
LP	Local interest (to be processed by IPv4 or IPv6 stack directly) or entry is resident in Pre-IFIB.

show lpts ifib

To display the entries in the Internal Forwarding Information Base (IFIB), use the **show lpts ifib** command in XR EXEC mode.

show lpts ifib [**entry**] [**type** {**bgp4** | **bgp6** | **isis** | **mcast4** | **mcast6** | **ospf-mc4** | **ospf-mc6** | **ospf4** | **ospf6** | **raw4** | **raw6** | **tcp4** | **tcp6** | **udp4** | **udp6**} | **all**] [**brief** [**statistics**]] [**slices**] [**times**] [**location** *node-id*]

Syntax Description

entry	(Optional) Displays the IFIB entries.
type	(Optional) Displays the following protocol types. • **bgp4** —IPv4 Border Gateway Protocol (BGP) slice • **bgp6** —IPv6 BGP slice • **isis** —Intermediate System-to-Intermediate System (IS-IS) slice • **mcast4** —IPv4 multicast slice • **mcast6** —IPv6 multicast slice • **ospf-mc4** —IPv4 Open Shortest Path First (OSPF) multicast slice • **ospf-mc6** —IPv6 OSPF multicast slice • **ospf4** —IPv4 OSPF slice • **ospf6** —IPv6 OSPF slice • **raw4** —IPv4 raw IP • **raw6** —IPv6 raw IP • **tcp4** —IPv4 Transmission Control Protocol (TCP) slice • **tcp6** —IPv6 TCP slice • **udp4** —IPv4 UDP slice • **udp6** —IPv6 UDP slice
all	Displays all IFIB types.
brief	(Optional) Displays the IFIB entries in brief format.
statistics	(Optional) Displays the IFIB table with statistics information.
slices	(Optional) Displays IFIB slices.
times	(Optional) Displays the IFIB update transaction times.
location *node-id*	(Optional) Specifies the location of the Flow Manager. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to display detailed information about the entries in an IFIB slice. This command is useful for debugging problems with delivering packets to applications.

When the **statistics** keyword is used, detailed statistics are displayed for packet count, number of entries in each slice, and a total entries count.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib** command:

```
RP/0/RP0/CPU0:router# show lpts ifib

O - Opcode; A - Accept Counter; D - Drop Counter; F - Flow Type; L - Listener Tag;
I - Local Flag; Y - SYN; T - Min TTL; DV - Deliver; DP - Drop; RE - Reassemble; na - Not
Applicable
----------------------------------------------------
VRF-ID            : default (0x60000000)
Port/Type         : any
Source Port       : any
Dest IP           : any
Source IP         : any
Layer 4           : 88 (88)
Interface         : any (0x0)
O/A/D/F/L/I/Y/T   : DELIVER/0/0/IPv4_STACK/0/0/0
Deliver List      : 0/5/CPU0
----------------------------------------------------
```

This table describes the significant fields shown in the display.

Table 40: show lpts ifib entries Command Field Descriptions

Field	Description
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Port/Type	Destination (local) TCP or UDP port number, or ICMP/IGMP packet type, or IPSec Security Parameters Index.t2222
Source Port	Source (remote) TCP or UDP port.
Dest IP	Destination (local) IP address.
Source IP	Source (remote) IP address.
Layer 4	Layer 4 protocol number (6 = TCP). **Note** Only the common Layer 4 protocol names are displayed.
Interface	Ingress interface name.

Field	Description
O/S/P/R/L/I/Y	• O: Opcode (DELIVER, DROP, or REASSEMBLE • S: Stats counter • P: Packet forwarding priority (LO, MED, or HIGH) • R: Rate limit (LO, MED, or HIGH) • L: Listener tag (IPv4_STACK, IPv6_STACK, or CLNL_STACK) • I: Local-interest flag (0 or 1) • Y: TCP SYN flag (0 or 1)
Deliver List	• (drop)—Drop packet • *rack/slot/module*—Deliver to single destination • [0xNNNN]—Deliver to multiple destinations (platform-dependent format)

The following sample output is from the **show lpts ifib brief** command:

```
RP/0/RP0/CPU0:router# show lpts ifib brief

 Slice    Local, Remote Address.Port            L4    Interface    Dlvr
 -------- ------------------------------------ ----- ------------ -----------
 TCP4     any.7 any                             TCP   any          0/RP1/CPU0
 TCP4     any.9 any                             TCP   any          0/RP1/CPU0
```

The following sample output is from the **show lpts ifib brief statistics** command:

```
RP/0/RP0/CPU0:router# show lpts ifib brief statistics

 Slice    Local, Remote Address.Port            L4    Interface    Accept/Drop
 -------- ------------------------------------ ----- ------------ -----------
 TCP4     any.7 any                             TCP   any          0/0
 TCP4     any.9 any                             TCP   any          0/0
 TCP4     any.19 any                            TCP   any          0/0

 Slice    Num. Entries Accepts/Drops
 -------- ------------ -------------
TCP4     3            0/0
Total    3            0/0
```

show lpts ifib slices

To display Internal Forwarding Information Base (IFIB) slice information, use the **show lpts ifib slices** command in XR EXEC mode.

show lpts ifib slices [**type** {**bgp4** | **bgp6** | **isis** | **mcast4** | **mcast6** | **ospf-mc4** | **ospf-mc6** | **ospf4** | **ospf6** | **raw4** | **raw6** | **tcp4** | **tcp6** | **udp4** | **udp6**}] [**all**] [**statistics**] [**times**]

Syntax Description

type	(Optional) Enter protocol types. • **bgp4** —IPv4 Border Gateway Protocol (BGP) slice • **bgp6** —IPv6 BGP slice • **isis** —Intermediate System-to-Intermediate System (IS-IS) slice • **mcast4** —IPv4 multicast slice • **mcast6** —IPv6 multicast slice • **ospf-mc4** —IPv4 Open Shortest Path First (OSPF) multicast slice • **ospf-mc6** —IPv6 OSPF multicast slice • **ospf4** —IPv4 OSPF slice • **ospf6** —IPv6 OSPF slice • **raw4** —IPv4 raw IP • **raw6** —IPv6 raw IP • **tcp4** —IPv4 Transmission Control Protocol (TCP) slice • **tcp6** —IPv6 TCP slice • **udp4** —IPv4 UDP slice • **udp6** —IPv6 UDP slice
all	(Optional) Displays all entries.
statistics	(Optional) Displays the statistics for slice lookups.
times	(Optional) Displays the IFIB update transaction times.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show lpts ifib slices** command when troubleshooting IFIB entries and slice assignments. This command is especially useful when troubleshooting problems with delivering packets to applications.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib slices** command:

```
RP/0/RP0/CPU0:router# show lpts ifib slices

Slice    L3   L4     Port  Location
-------- ---- ------ ----- --------
RAWIP4   IPV4 any    any   0/RP0/CPU0
RAWIP6   IPV6 any    any   0/RP0/CPU0
OSPF4    IPV4 OSPF   any   0/RP0/CPU0
OSPF6    IPV6 OSPF   any   0/RP0/CPU0
OSPF_MC4 IPV4 any    any   0/RP0/CPU0
OSPF_MC6 IPV6 any    any   0/RP0/CPU0
BGP4     IPV4 TCP    179   0/RP0/CPU0
BGP6     IPV6 TCP    179   0/RP0/CPU0

UDP4     IPV4 UDP    any   0/RP0/CPU0
UDP6     IPV6 UDP    any   0/RP0/CPU0
TCP4     IPV4 TCP    any   0/RP0/CPU0
TCP6     IPV6 TCP    any   0/RP0/CPU0
ISIS     CLNS -      any   0/RP0/CPU0
MCAST4   IPV4 any    any   0/RP0/CPU0
MCAST6   IPV6 any    any   0/RP0/CPU0
```

The following sample output is from the **show lpts ifib slices times** command:

```
RP/0/RP0/CPU0:router# show lpts ifib slices times

Slice    L3   L4     Port  Location
-------- ---- ------ ----- --------
RAWIP4   IPV4 any    any   0/RP0/CPU0
RAWIP6   IPV6 any    any   0/RP0/CPU0
OSPF4    IPV4 OSPF   any   0/RP0/CPU0
OSPF6    IPV6 OSPF   any   0/RP0/CPU0
OSPF_MC4 IPV4 any    any   0/RP0/CPU0
OSPF_MC6 IPV6 any    any   0/RP0/CPU0
BGP4     IPV4 TCP    179   0/RP0/CPU0
BGP6     IPV6 TCP    179   0/RP0/CPU0

UDP4     IPV4 UDP    any   0/RP0/CPU0
UDP6     IPV6 UDP    any   0/RP0/CPU0
TCP4     IPV4 TCP    any   0/RP0/CPU0
TCP6     IPV6 TCP    any   0/RP0/CPU0
ISIS     CLNS -      any   0/RP0/CPU0
MCAST4   IPV4 any    any   0/RP0/CPU0
MCAST6   IPV6 any    any   0/RP0/CPU0
  Flow Manager 0/RP0/CPU0:
   total:5 tx 13 upd 1/-/1ms/tx
```

The following sample output is from the **show lpts ifib slices statistics** command:

```
RP/0/RP0/CPU0:router# show lpts ifib slices all statistics

Slice    L3   L4     Port  Location   Lookups RmtDlvr Rejects RLDrops NoEntry
```

```
-------- ---- ------ ----- ---------- ------- ------- ------- ------- -------
RAWIP4   IPV4 any    any   0/0/CPU0   5       0       0       0       0
RAWIP6   IPV6 any    any   0/0/CPU0   0       0       0       0       0
OSPF4    IPV4 OSPF   any   0/0/CPU0   0       0       0       0       0
OSPF6    IPV6 OSPF   any   0/0/CPU0   0       0       0       0       0
OSPF_MC4 IPV4 any    any   0/0/CPU0   0       0       0       0       0
OSPF_MC6 IPV6 any    any   0/0/CPU0   0       0       0       0       0
BGP4     IPV4 TCP    179   0/0/CPU0   0       0       0       0       0
BGP6     IPV6 TCP    179   0/0/CPU0   0       0       0       0       0

UDP4     IPV4 UDP    any   0/0/CPU0   3704    0       979     0       0
UDP6     IPV6 UDP    any   0/0/CPU0   0       0       0       0       0
TCP4     IPV4 TCP    any   0/0/CPU0   0       0       0       0       0
TCP6     IPV6 TCP    any   0/0/CPU0   0       0       0       0       0
ISIS     CLNS -      any   0/0/CPU0   0       0       0       0       0
MCAST4   IPV4 any    any   0/0/CPU0   0       0       0       0       0
MCAST6   IPV6 any    any   0/0/CPU0   0       0       0       0       0
  Flow Manager 0/0/CPU0:
   Packets in: 3792
   Packets delivered locally without lookups: 83
   Slice lookups: 3709
     Rejects: 979
```

This table describes the significant fields shown in the display.

Table 41: show lpts ifib slices statistics Command Field Descriptions

Field	Description
Slice	Slice number.
L3-proto	Layer 3 protocol (IPv4, IPv6, CLNL).
L4-proto	Layer 4 protocol (TCP, UDP, and others).
Port	Local (destination) TCP or UDP port.
Location	Node location, in the format *rack/slot/module*.

show lpts ifib statistics

To display Internal Forwarding Information Base (IFIB) statistics, use the **show lpts ifib statistics** command in .

show lpts ifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib statistics** command:

```
RP/0/# show lpts ifib statistics

Flow Manager 0/RP0/CPU0:
   Packets in:254
   Packets delivered locally without lookups:0
   Slice lookups:254
     Post-lookup error drops:
      Failed ipv4_netio_input:1
     Rejects:254
    Packets delivered locally:0
    Packets delivered remotely:0
```

This table describes the significant fields shown in the display.

Table 42: show lpts ifib statistics Command Field Descriptions

Field	Description
Packets in	Packets presented to the LPTS decaps node in netio.
Packets delivered locally without lookups	Packets previously resolved on a LC delivered directly to L3.
Slice lookups	Packets requiring slice lookups.

Field	Description
Post-lookup error drops	Packets dropped after a slice lookup.
Rejects	Packets that caused a TCP RST or ICMP Port/Protocol Unreachable.
Packets delivered locally	Packets delivered to local applications after slice lookups.
Packets delivered remotely	Packets delivered to applications on remote RPs.

Note The sample output is an example only and displays only those fields showing a value. No display exists for nonzero values. This command may show other values depending on your router configuration.

show lpts ifib times

To display Internal Forwarding Information Base (IFIB) update transaction times, use the **show lpts ifib times** command in XR EXEC mode.

show lpts ifib times [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays IFIB update transaction times for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts ifib times** command:

```
RP/0/RP0/CPU0:router# show lpts ifib times

Slice    L3   L4     Port  Location
-------- ---- ------ ----- --------
RAWIP4   IPV4 any    any   0/RP1/CPU0
RAWIP6   IPV6 any    any   0/RP1/CPU0
OSPF4    IPV4 OSPF   any   0/RP1/CPU0
OSPF6    IPV6 OSPF   any   0/RP1/CPU0
OSPF_MC4 IPV4 any    any   0/RP1/CPU0
OSPF_MC6 IPV6 any    any   0/RP1/CPU0
BGP4     IPV4 TCP    179   0/RP1/CPU0
BGP6     IPV6 TCP    179   0/RP1/CPU0
UDP4     IPV4 UDP    any   0/RP1/CPU0
UDP6     IPV6 UDP    any   0/RP1/CPU0
TCP4     IPV4 TCP    any   0/RP1/CPU0
TCP6     IPV6 TCP    any   0/RP1/CPU0
ISIS     CLNS -      any   0/RP1/CPU0
MCAST4   IPV4 any    any   0/RP1/CPU0
MCAST6   IPV6 any    any   0/RP1/CPU0
Flow Manager 0/RP0/CPU0:
 total:5 tx 13 upd 1/-/1ms/tx
```

This table describes the significant fields shown in the display.

Table 43: show lpts ifib times Command Field Descriptions

Field	Description
Slice	Slice number.
L3 Protocol	Layer 3 protocol (IPv4, IPV6, CLNL).
L4 Protocol	Layer 4 protocol (TCP, UDP, and so on).
Port	Local (destination) TCP or UDP port.
Location	Node location, in the format *rack/slot/module*.

show lpts pifib

To display Pre-Internal Forwarding Information Base (Pre-IFIB) entries, use the **show lpts pifib** command in XR EXEC mode.

show lpts pifib [entry] [hardware {**entry | police**} [**brief**] **[location** *node-id*]

Syntax Description

entry	(Optional) Pre-IFIB entry.
hardware	(Optional) Displays hardware for Pre-IFIB.
entry	(Optional) Displays the entries for Pre-IFIB.
police	(Optional) Displays the policer values that are being use.
brief	(Optional) Pre-IFIB entries in brief format.
location *node-id*	(Optional) The *node-id* argument is entered in the *rack/slot/module* notation (for example, 0/7/CPU0).

Command Default

By default, all entries are displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show lpts pifib** command with the **brief** keyword to perform the following functions:

- Display entries of all or part of a Pre-IFIB.
- Display a short description of each entry in the LPTS Pre-IFIB, optionally displaying packet counts for each entry.

Note These statistics are used only for packets that are processed by a line card, route processor, or distributed route processor.

Pre-IFIB statistics for packets processed by line card hardware are counted separately.

By default, all the defaults including the statistics for **hardware** are displayed.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output for the **show lpts pifib** command:

```
RP/0/RP0/CPU0:router#  show lpts pifib entry brief location 0/3/CPU0

* - Any VRF; I - Local Interest;
X - Drop; R - Reassemble;

 Type       VRF-ID   L4     Interface    Deliver      Local-Address,Port Remote-Address,Port

 ---------- -------- ------ ------------ ------------ --------------------------------------

 ISIS       *        -      any          0/RP0/CPU0   - -
 IPv4_frag  *        any    any          R             any any
 IPv4_echo  *        ICMP   any          I             any,ECHO any
 IPv4       *        ICMP   any          0/RP0/CPU0   any,ECHOREPLY any
 IPv4       *        ICMP   any          I             any,TSTAMP any
 IPv4       *        ICMP   any          I            any,MASKREQ any
 IPv4       *        TCP    any          0/RP0/CPU0   any any,179
 IPv4       *        TCP    any          0/RP0/CPU0   any,179 any
 IPv4       *        TCP    any          0/RP0/CPU0   any any
 IPv4       *        UDP    any          0/RP0/CPU0   any,1701 any
 IPv4       *        UDP    any          0/RP0/CPU0   any any
 IPv4       *        OSPF   any          0/RP0/CPU0   192.0.0.5 any
 IPv4       *        OSPF   any          0/RP0/CPU0   192.0.0.6 any
 IPv4       *        OSPF   any          0/RP0/CPU0   any any
 IPv4       *        any    any          0/RP0/CPU0   any any
 IPv6_frag  *        any    any          R             any any
 IPv6_echo  *        ICMP6  any          I            any,ECHOREQ any
```

The following is sample output for the **show lpts pifib type** command using the **ipv4** and **tcp** keywords.

```
RP/0/RP0/CPU0:router# show lpts pifib type ipv4 tcp

O - Opcode; F - Flow Type; L - Listener Tag; I - Local Flag; T - Min TTL;
na - Not Applicable
----------------------------------------------------
L3 Protocol       : IPV4
L4 Protocol       : TCP
VRF-ID            : default (0x60000000)
Destination IP    : any
Source IP         : any
Port/Type         : Port:23
Source Port       : any
Is Fragment       : 0
Is SYN            : 0
Interface         : any (0x0)
O/F/L/I/T         : DELIVER/TELNET-default/IPv4_LISTENER/0/0
Deliver List      : 0/RP0

/CPU0
Accepts/Drops     : 0/0
Is Stale          : 0
----------------------------------------------------
```

The following is sample output from the **show lpts pifib** command with the **entry** and **brief** keywords added command:

```
RP/0/RP0/CPU0:router# show lpts pifib entry brief
```

```
* - Critical Flow; I - Local Interest;
X - Drop; R - Reassemble;

 Type       VRF-ID   Local, Remote Address.Port L4    Interface    Deliver
 ---------- -------- -------------------------- ----- ------------ -------------

 ISIS       *        - -                        -     any          0/0/CPU0
 IPv4_frag  *        any any                    any   any          R
 IPv4_IXMP  *        any.ECHO any               ICMP  any          XI
 IPv4_IXMP  *        any.TSTAMP any             ICMP  any          XI
 IPv4_IXMP  *        any.MASKREQ any            ICMP  any          XI
 IPv4_IXMP  *        any any                    ICMP  any          0/0/CPU0
 IPv4_IXMP  *        any any                    IGMP  any          0/0/CPU0
 IPv4_mcast *        192.0.0.5 any              any   any          0/0/CPU0
 IPv4_mcast *        192.0.0.6 any              any   any          0/0/CPU0
 IPv4_mcast *        192.0.0.0/4 any            any   any          0/0/CPU0

 IPv4_TCP   *        any.179 any                TCP   any          0/0/CPU0
 IPv4_TCP   *        any any.179                TCP   any          0/0/CPU0
 IPv4_TCP   *        any any                    TCP   any          0/0/CPU0
 IPv4_UDP   *        any any                    UDP   any          0/0/CPU0
 IPv4_IPsec *        any any                    ESP   any          0/0/CPU0
 IPv4_IPsec *        any any                    AH    any          0/0/CPU0
 IPv4_rawIP *        any any                    OSPF  any          0/0/CPU0
 IPv4_rawIP *        any any                    any   any          0/0/CPU0
 IPv6_frag  *        any any                    any   any          R
 IPv6_ICMP  *        any.na any                 ICMP6 any          XI
 IPv6_ICMP  *        any any                    ICMP6 any          0/0/CPU0
 IPv6_mcast *        ff02::5 any                any   any          0/0/CPU0
 IPv6_mcast *        ff02::6 any                any   any          0/0/CPU0
 IPv6_mcast *        ff00::/8 any               any   any          0/0/CPU0
 IPv6_TCP   *        any.179 any                TCP   any          0/0/CPU0
 IPv6_TCP   *        any any.179                TCP   any          0/0/CPU0
 IPv6_TCP   *        any any                    TCP   any          0/0/CPU0
 IPv6_UDP   *        any any                    UDP   any          0/0/CPU0
 IPv6_IPsec *        any any                    ESP   any          0/0/CPU0
 IPv6_IPsec *        any any                    AH    any          0/0/CPU0
 IPv6_rawIP *        any any                    OSPF  any          0/0/CPU0
 IPv6_rawIP *        any any                    any   any          0/0/CPU0
```

The following sample output is from the **show lpts pifib** command with the **entry, brief,** and **entry brief statistics** keywords added:

```
RP/0/RP0/CPU0:router# show lpts pifib entry brief statistics

* - Critical Flow; I - Local Interest;
X - Drop; R - Reassemble;

 Type       VRF-ID   Local, Remote Address.Port L4    Interface    Accepts/Drops

 ---------- -------- -------------------------- ----- ------------ -------------

 ISIS       *        - -                        -     any          0/0
 IPv4_frag  *        any any                    any   any          0/0
 IPv4_IXMP  *        any.ECHO any               ICMP  any          0/0
 IPv4_IXMP  *        any.TSTAMP any             ICMP  any          0/0
 IPv4_IXMP  *        any.MASKREQ any            ICMP  any          0/0
 IPv4_IXMP  *        any any                    ICMP  any          5/0
 IPv4_IXMP  *        any any                    IGMP  any          0/0
 IPv4_mcast *        224.0.0.5 any              any   any          0/0
 IPv4_mcast *        224.0.0.6 any              any   any          0/0
 IPv4_mcast *        224.0.0.0/4 any            any   any          0/0
 IPv4_TCP   *        any.179 any                TCP   any          0/0
 IPv4_TCP   *        any any.179                TCP   any          0/0
 IPv4_TCP   *        any any                    TCP   any          0/0
 IPv4_UDP   *        any any                    UDP   any          4152/0
 IPv4_IPsec *        any any                    ESP   any          0/0
 IPv4_IPsec *        any any                    AH    any          0/0
 IPv4_rawIP *        any any                    OSPF  any          0/0

-----------------

statistics:

Type            Num. Entries         Accepts/Drops

------          ------------         -------------
ISIS            1                    0/0
IPv4_frag       1                    0/0
IPv4_IXMP       5                    5/0
IPv4_mcast      3                    0/0
IPv4_TCP        3                    0/0
IPv4_UDP        1                    4175/0
IPv4_IPsec      2                    0/0
IPv4_rawIP      2                    0/0
IPv6_frag       1                    0/0
IPv6_ICMP       2                    0/0
IPv6_mcast      3                    0/0
IPv6_TCP        3                    0/0
IPv6_UDP        1                    0/0
IPv6_IPsec      2                    0/0
IPv6_rawIP      2                    0/0
Total           32

Packets into Pre-IFIB: 4263
Lookups: 4263
Packets delivered locally: 4263
Packets delivered remotely: 0
```

This table describes the significant fields shown in the display for the **show lpts pifib** command with the **brief** and **statistics** keywords .

Table 44: show lpts pifib Command Field Descriptions

Field	Description
Type	Hardware entry type.
VRF ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Local, Remote Address. Port	Indicates local address (in the form of local port and type) and remote address (remote port).
L4	Layer 4 protocol of the entry.
Interface	Interface for this entry.
Accepts/Drops	Number of packets sent to DestAddr/Number of packets dropped due to policing.

Field	Description
Num. Entries	Number of pre-ifib entries of the listed type.
Packets into Pre-IFIB	Packets presented for pre-IFIB lookups.
Lookups	Packets looked up.
Packets delivered locally	Packets delivered to local applications or the local stack (*n* duplicated) packets duplicated for delivery to applications and the local stack.
Packets delivered remotely	Packets delivered to applications or for lookup on other RPs.

show lpts pifib hardware entry

To display entries in the Local Packet Transport Services (LPTS) pre-IFIB hardware table, use the **show lpts pifib hardware entry** command in XR EXEC mode.

show lpts pifib hardware entry [**brief**] [**location** {**all***node_id*}]

Syntax Description

brief	(Optional) Displays summary hardware entry information.
location all	(Optional) Specifies all locations.
location *node-id*	(Optional) Displays pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

Displays hardware entry information in brief.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts pifib hardware entry** command with the **location** keyword:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware entry brief location 0/3/CPU0

* - Read on clear stats
----------------------------------------------------

DestIP             L4Proto  port/Type          remotePort    npu    ListenerTag
Flowtype                DestNode           Accepted* Dropped*
------------------ -----    ------------------ ------------- ------ ------------------
------------------      ------------------ --------- ---------
0.0.0.0            0        any                0             0      IPv4_REASS
Fragment                Local LC           0         0
0.0.0.0            1        ICMP_Dflt          0             0      RAWIP4_FM
ICMP-default            Local LC           0         0
192.0.0.5          89       any                0             0      IPv4_STACK
OSPF-mc-default         Deliver RP         72        0
192.0.0.6          89       any                0             0      IPv4_STACK
OSPF-mc-default         Deliver RP         0         0
0.0.0.0            89       any                0             0      OSPF4_FM
```

```
OSPF-uc-default         Deliver RP         30        0
0.0.0.0            6        Port:179          0             0      BGP4_FM
BGP-default             Local LC           0         0
0.0.0.0            6        Port:any          179           0      BGP4_FM
BGP-default             Local LC           25        0
0.0.0.0            6        Port:any          0             0      TCP4_FM
TCP-default             Local LC           0         0
0.0.0.0            17       Port:any          0             0      UDP4_FM
UDP-default             Local LC           67        0
0.0.0.0            46       any               0             0      RAWIP4_FM
RSVP-default            Local LC           0         0
0.0.0.0            0        any               0             0      RAWIP4_FM
Raw-default             Local LC           0         0
::                 0        any               0             0      IPv6_REASS
Fragment                Local LC           0         0
::                 58       ICMP6_LL          0             0      RAWIP6_FM
ICMP-default            Local LC           10        0
::                 58       ICMP6_MD          0             0      RAWIP6_FM
ICMP-default            Local LC           3         0
::                 58       ICMP6_Dflt        0             0      RAWIP6_FM
ICMP-default            Local LC           4         0
2001:DB8::1        89       any               0             0      IPv6_STACK
OSPF-mc-default         Deliver RP         76        0
2001:DB8::2        89       any               0             0      IPv6_STACK
OSPF-mc-default         Deliver RP         0         0
::                 89       any               0             0      OSPF6_FM
OSPF-uc-default         Deliver RP         44        0
::                 6        Port:179          0             0      BGP6_FM
BGP-default             Local LC           16        0
::                 6        Port:any          179           0      BGP6_FM
BGP-default             Local LC           16        0
::                 6        Port:any          0             0      TCP6_FM
TCP-default             Local LC           0         0
::                 17       Port:any          0             0      UDP6_FM
UDP-default             Local LC           0         0
::                 0        any               0             0      RAWIP6_FM
Raw-default             Local LC           0         0
any                0        ISIS_Dflt         0             0      CLNS_STACK
ISIS-default            Deliver RP         56        0
any                0        ISIS_Jumbo        0             0      CLNS_STACK
ISIS-default            Deliver RP         0         0
```

This table describes the significant fields shown in the display.

Table 45: show lpts pifib hardware entry Command Field Descriptions

Field	Description
DestIP	IP address of the destination node.
L4 Protocol	Layer 4 protocol of the entry.
Port/Type	Port or type for this entry.
remotePort	Remote port for this entry.
npu	Network Processor Unit.
ListenerTag	Name of the listener node.
Flowtype	Type of the LPTS flow.

Field	Description
DestNode	Destination node to which to send the packet.
Accepted/Dropped	Number of packets sent to DestAddr/Number of packets dropped due to policing.

show lpts pifib hardware object-group entry

To display OGLPTS (Object-Group LPTS) entries that accommodate higher number of BGP sessions for BGP peering, use the **show lpts pifib hardware object-group entry** command in XR EXEC mode.

show lpts pifib hardware object-group entry [**brief**] [**location** { **all** *node_id* }]

Syntax Description

object-group entry	Displays the OGLPTS entries for BGP sessions.
brief	(Optional) Displays summary of hardware entry information.
location all	(Optional) Specifies all locations.
location *node-id*	(Optional) Displays pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

Displays hardware entry information in brief.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

This sample output is from the **show lpts pifib hardware object-group entry brief location all** command that shows summary of all the OGLPTS entries in brief:

```
Router# show lpts pifib hardware object-group entry brief location all
Wed Jan  6 19:54:44.012 UTC

-----------------------------------------------------------------------

Type DestIP               DestOgid   SrcIP                SrcOgid    Interface          vrf
   L4   LPort/Type   RPort  npu  Flowtype           DestNode     PuntPrio        Accept
Drop
---- -------------------- --------   -------------------- --------   --------------
----- ---  ------------ ------ ---- ------------------ --------      ------------   ------
  ------
IPv4 123.123.123.2        1025       123.123.123.1        1          any                 1
    6    Port:179     42319  0    BGP-known          Dlvr RP0     CRITICAL        0
0
IPv4 123.123.123.2        1025       123.123.123.1        1          any                 1
```

```
    6    Port:179     0      0    BGP-cfg-peer       Dlvr RP0     MEDIUM         0
0
IPv4 any                  any        any                  any        any                0
    6    Port:any     179    0    BGP-default        Dlvr RP0     LOW            0
0
IPv4 any                  any        any                  any        any                0
    6    Port:179     0      0    BGP-default        Dlvr RP0     LOW            0
0
IPv6 123::2               1025       123::1               1          any                1
    6    Port:179     39330  0    BGP-known          Dlvr RP0     CRITICAL       0
0
IPv6 123::2               1025       123::1               1          any                1
    6    Port:179     0      0    BGP-cfg-peer       Dlvr RP0     MEDIUM         0
0
IPv6 any                  any        any                  any        any                0
    6    Port:any     179    0    BGP-default        Dlvr RP0     LOW            0
0
IPv6 any                  any        any                  any        any                0
    6    Port:179     0      0    BGP-default        Dlvr RP0     LOW            0
0
```

This table describes the significant fields shown in the display.

Table 46: show lpts pifib hardware object-group entry brief location all Command Output Field Descriptions

Field	Description
DestIP	IP address of the destination node.
DestOgid	ID of the object-group entry for the destination node.
SrcIP	IP address of the source node.
SrcOgId	ID of the object-group entry for the source node.
Interface	Interface of the BGP session
vrf	VRF ID
L4	Layer 4 protocol of the object-group entry.
LPort/Type	Port or type for this object-group entry.
RPort	Remote port for this object-group entry.
npu	Network Processor Unit.
Flowtype	Type of the LPTS flow.
ListenerTag	Name of the listener node.
DestNode	Destination node to which to send the packet.

Field	Description
PuntPrio	Punt priority of the LPTS packet. The values of PuntPrio can be Critical, High, Medium, or Low.
Accepted/Dropped	Number of packets sent to DestAddr/Number of packets dropped due to policing.

This sample output is from the **show lpts pifib hardware object-group entry location all** command that shows all the OGLPTS entries in details:

```
Router# show lpts pifib hardware object-group entry location all
Wed Jan  6 19:55:08.871 UTC

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 42319
npu id            : 0
Destination IP    : 123.123.123.2
Source IP         : 123.123.123.1
DestOgid          : 1025
SrcOgid           : 1
Port/Type         : Port:179
Is Fragment       : 0
vrf               : 1
Listener Tag      : IPv4_STACK
Flow Type         : BGP-known
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : CRITICAL
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 0
npu id            : 0
Destination IP    : 123.123.123.2
Source IP         : 123.123.123.1
DestOgid          : 1025
SrcOgid           : 1
Port/Type         : Port:179
Is Fragment       : 0
vrf               : 1
Listener Tag      : IPv4_LISTENER
Flow Type         : BGP-cfg-peer
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : MEDIUM
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 179
npu id            : 0
Destination IP    : any
Source IP         : any
```

```
DestOgid          : any
SrcOgid           : any
Port/Type         : Port:any
Is Fragment       : 0
vrf               : 0
Listener Tag      : BGP4_FM
Flow Type         : BGP-default
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : LOW
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 0
npu id            : 0
Destination IP    : any
Source IP         : any
DestOgid          : any
SrcOgid           : any
Port/Type         : Port:179
Is Fragment       : 0
vrf               : 0
Listener Tag      : BGP4_FM
Flow Type         : BGP-default
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : LOW
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 39330
npu id            : 0
Destination IP    : 123::2
Source IP         : 123::1
DestOgid          : 1025
SrcOgid           : 1
Port/Type         : Port:179
Is Fragment       : 0
vrf               : 1
Listener Tag      : IPv6_STACK
Flow Type         : BGP-known
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : CRITICAL
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 0
npu id            : 0
Destination IP    : 123::2
Source IP         : 123::1
DestOgid          : 1025
SrcOgid           : 1
Port/Type         : Port:179
Is Fragment       : 0
vrf               : 1
Listener Tag      : IPv6_LISTENER
Flow Type         : BGP-cfg-peer
```

```
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : MEDIUM
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 179
npu id            : 0
Destination IP    : any
Source IP         : any
DestOgid          : any
SrcOgid           : any
Port/Type         : Port:any
Is Fragment       : 0
vrf               : 0
Listener Tag      : BGP6_FM
Flow Type         : BGP-default
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : LOW
Interface         : any
Accepted/Dropped  : 0/0

----------------------------------------------------
L4 Protocol       : 6
L4 remote port    : 0
npu id            : 0
Destination IP    : any
Source IP         : any
DestOgid          : any
SrcOgid           : any
Port/Type         : Port:179
Is Fragment       : 0
vrf               : 0
Listener Tag      : BGP6_FM
Flow Type         : BGP-default
DestNode          : Deliver RP0
Type              : Dlvr
Punt Queue Prio   : LOW
Interface         : any
Accepted/Dropped  : 0/0
```

show lpts pifib hardware police

To display the policer configuration value set, use the **show lpts pifib hardware police** command in XR EXEC mode.

show lpts pifib hardware police [**location** {**all***node-id*}]

Syntax Description

location *node-id*	(Optional) Displays pre-Internal Forwarding Information Base (IFIB) information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
all	Specifies all locations.

Command Default

If no policer is configured, the default value is the configured rate.

Command Modes

XR EXEC mode

Command History

Release	**Modification**
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Note Cisco IOS XR Release 7.3.2 introduces support to monitor LPTS host path drops via `Cisco-IOS-XR-lpts-pre-ifib-oper` YANG data model.

Task ID

Task ID	**Operations**
lpts	read

Examples

This sample output is from the **show lpts pifib hardware police** command with the **location** keyword for 0/0/CPU0:

```
Router#show lpts pifib hardware police location 0/0/CPU0

-------------------------------------------------------------
                Node 0/0/CPU0:
-------------------------------------------------------------
FlowType               Policer Type    Cur. Rate Burst     Accepted     Dropped      npu

--------------------- ------- ------- --------- --------- ------------ ------------ ---------
Fragment               2       np      542       1000      0            0            0

Fragment               2       np      542       1000      0            0            1

OSPF-mc-known          3       np      1627      1000      0            0            0
```

```
OSPF-mc-known          3       np      1627      1000      0            0            1
OSPF-mc-default        4       np      1084      1000      0            0            0
OSPF-mc-default        4       np      1084      1000      0            0            1
OSPF-uc-known          5       np      542       1000      0            0            0
OSPF-uc-known          5       np      542       1000      0            0            1
OSPF-uc-default        6       np      542       1000      0            0            0
OSPF-uc-default        6       np      542       1000      0            0            1
BFD-default            10      np      8136      1000      0            0            0
BFD-default            10      np      8136      1000      0            0            1
BFD-MP-known           11      np      8136      1000      0            0            0
BFD-MP-known           11      np      8136      1000      0            0            1
BGP-known              16      np      9763      1000      0            0            0
BGP-known              16      np      9763      1000      0            0            1
BGP-cfg-peer           17      np      1084      1000      0            0            0
BGP-cfg-peer           17      np      1084      1000      0            0            1
BGP-default            18      np      542       1000      0            0            0
BGP-default            18      np      542       1000      0            0            1
PIM-mcast-default      19      np      542       1000      0            0            0
PIM-mcast-default      19      np      542       1000      0            0            1
PIM-mcast-known        20      np      1627      1000      0            0            0
PIM-mcast-known        20      np      1627      1000      0            0            1
PIM-ucast              21      np      542       1000      0            0            0
PIM-ucast              21      np      542       1000      0            0            1
IGMP                   22      np      1627      1000      0            0            0
IGMP                   22      np      1627      1000      0            0            1
ICMP-local             23      np      542       1000      0            0            0
ICMP-local             23      np      542       1000      0            0            1
ICMP-control           25      np      2169      1000      0            0            0
ICMP-control           25      np      2169      1000      0            0            1
LDP-TCP-known          28      np      2169      1000      0            0            0
LDP-TCP-known          28      np      2169      1000      0            0            1
LDP-TCP-cfg-peer       29      np      1084      1000      0            0            0
```

```
LDP-TCP-cfg-peer       29      np      1084      1000      0            0            1
LDP-TCP-default        30      np      542       1000      0            0            0
LDP-TCP-default        30      np      542       1000      0            0            1
LDP-UDP                31      np      542       1000      0            0            0
LDP-UDP                31      np      542       1000      0            0            1
All-routers            32      np      542       1000      0            0            0
All-routers            32      np      542       1000      0            0            1
RSVP-default           38      np      542       1000      0            0            0
RSVP-default           38      np      542       1000      0            0            1
RSVP-known             39      np      1627      1000      0            0            0
RSVP-known             39      np      1627      1000      0            0            1
SNMP                   47      np      542       1000      0            0            0
SNMP                   47      np      542       1000      0            0            1
SSH-known              48      np      542       1000      0            0            0
SSH-known              48      np      542       1000      0            0            1
SSH-default            49      np      542       1000      0            0            0
SSH-default            49      np      542       1000      0            0            1
HTTP-known             50      np      542       1000      0            0            0
HTTP-known             50      np      542       1000      0            0            1
SHTTP-known            52      np      542       1000      0            0            0
SHTTP-known            52      np      542       1000      0            0            1
TELNET-known           54      np      542       1000      0            0            0
TELNET-known           54      np      542       1000      0            0            1
TELNET-default         55      np      542       1000      0            0            0
TELNET-default         55      np      542       1000      0            0            1
UDP-known              60      np      24950     1000      0            0            0
UDP-known              60      np      24950     1000      0            0            1
UDP-default            63      np      542       1000      0            0            0
UDP-default            63      np      542       1000      0            0            1
TCP-default            67      np      542       1000      0            0            0
TCP-default            67      np      542       1000      0            0            1
Raw-default            71      np      542       1000      0            0            0
```

```
Raw-default            71      np      542       1000      0            0            1
GRE                    77      np      542       1000      0            0            0
GRE                    77      np      542       1000      0            0            1
VRRP                   78      np      542       1000      0            0            0
VRRP                   78      np      542       1000      0            0            1
DNS                    83      np      542       1000      0            0            0
DNS                    83      np      542       1000      0            0            1
NTP-known              87      np      542       1000      0            0            0
NTP-known              87      np      542       1000      0            0            1
DHCPv4                 93      np      3796      1000      0            0            0
DHCPv4                 93      np      3796      1000      0            0            1
DHCPv6                 94      np      3796      1000      0            0            0
DHCPv6                 94      np      3796      1000      0            0            1
TPA                    96      np      1627      1000      0            0            0
TPA                    96      np      1627      1000      0            0            1
PM-TWAMP               99      np      1627      1000      0            0            0
PM-TWAMP               99      np      1627      1000      0            0            1
```

This table describes the significant fields shown in the display.

Table 47: show lpts pifib hardware police Command Field Descriptions

FIeld	Description
FlowType	Type of flow that is binding between a tuple and a destination.
Policer	Policer Values in PPS.
Type	Type of LPTS entry.
Cur. Rate	Packet rate effective in hardware for the entry.
Burst	Accepable burst size for the policer.
npu	Network Processor Unit.

show lpts pifib statistics

To display Pre-Internal Forwarding Information Base (Pre-IFIB) statistics, use the **show lpts ifib statistics** command in XR EXEC mode.

show lpts pifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays Pre-IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts pifib statistics** command:

```
RP/0/RP0/CPU0:router# show lpts pifib statistics

Packets into Pre-IFIB:80
Lookups:80
Packets delivered locally:80
Packets delivered remotely:0
```

This table describes the significant fields shown in the display.

Table 48: show lpts pifib statistics Command Field Descriptions

Field	Description
Packets into Pre-IFIB	Packets presented for pre-IFIB lookups.
Lookups	Packets looked up.
Packets delivered locally	Packets delivered to local applications or the local stack (*n* duplicated) packets duplicated for delivery to applications and the local stack.
Packets delivered remotely	Packets delivered to applications or for lookup on other RPs.

show lpts port-arbitrator statistics

To display local packet transport services (LPTS) port arbitrator statistics, use the **show lpts port-arbitrator statistics** command in XR EXEC mode.

show lpts port-arbitrator statistics

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts port-arbitrator statistics** command:

```
RP/0/RP0/CPU0:router# show lpts port-arbitrator statistics

LPTS Port Arbitrator statistics:
 PA FGID-DB library statistics:
  0 FGIDs in use, 512 cached, 0 pending retries
  0 free allocation slots, 0 internal errors, 0 retry attempts
  1 FGID-DB notify callback, 0 FGID-DB errors returned
  FGID-DB permit mask: 0x7 (alloc mark rack0)
  PA API calls:
            1 init              1 realloc_done
            8 alloc             8 free
           16 join             16 leave
            8 detach
  FGID-DB API calls:
            1 register          1 clear_old
            1 alloc             0 free
           16 join             16 leave
            0 mark              1 mark_done
```

show lpts vrf

To display the Local Packet Transport Services (LPTS) VPN routing and forwarding (VRF) instance identification numbers and names, use the **show lpts vrf** command in XR EXEC mode.

show lpts vrf

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
lpts	read

Examples

The following sample output is from the **show lpts vrf** command:

```
RP/0/RP0/CPU0:router# show lpts vrf

VRF-ID      VRF-NAME
0x00000000  *
0x60000000  default
```

This table describes the significant fields shown in the display.

Table 49: show lpts vrf Command Field Descriptions

Field	Description
VRF-ID	VPN routing and forwarding (VRF) identification (vrfid) number.
VRF-NAME	Name given to the VRF.

Network Stack Commands

This chapter describes the Cisco IOS XR softwareto configure and monitor features related to IP Version 4 (IPv4) and IP Version 6 (IPv6).

For detailed information about network stack concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries, use the **clear ipv6 neighbors** command in XR EXEC mode.

clear ipv6 neighbors [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) The designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	
Release 7.0.12	This command was introduced.

Usage Guidelines

If the location option is specified, only the neighbor entries specified in the **location** *node-id* keyword and argument are cleared.

Task ID

Task ID	Operations
network	read, write
IPv6	execute

Examples

In the following example, only the highlighted entry is deleted:

```
RP/0/RP0/CPU0:router# clear ipv6 neighbors ?
location specify a node name

RP/0/RP0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH HundredGigE0/0/0/0
8888::8 - 1234.2345.9877 REACH HundredGigE0/0/0/0
fe80::205:1ff:fe9f:6400 1335 0005.019f.6400 STALE HundredGigE0/0/0/0
fe80::206:d6ff:fece:3808 1482 0006.d6ce.3808 STALE HundredGigE0/0/0/0
fe80::200:11ff:fe11:1112 1533 0000.1111.1112 STALE HundredGigE0/0/0/2

RP/0/RP0/CPU0:router# clear ipv6 neighbors location 0/2/0
RP/0/RP0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH HundredGigE0/0/0/0
8888::8 - 1234.2345.9877 REACH HundredGigE0/0/0/0
fe80::205:1ff:fe9f:6400 1387 0005.019f.6400 STALE HundredGigE0/0/0/0
```

```
fe80::206:d6ff:fece:3808 1534 0006.d6ce.3808 STALE HundredGigE0/0/0/0
```

clear ipv6 path-mtu

To clear the learnt path maximum transmission unit (MTU) values of IPv6 packets, use the **clear ipv6 path-mtu** command in the XR EXEC mode.

clear ipv6 path-mtu [**vrf** {*vrf-name* | **all**} [**location** *node-id*]] [**address** { *ipv6-address* } [**location** *node-id*]]

Syntax Description

location *node-id*	(Optional) The designated node. The node-id argument is entered in the *rack/slot/module* notation.
ipv6-address	(Optional) Specific IPv6 address.

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If the location option is specified, only the entries of the node specified in the **location** *node-id* keyword and argument are cleared. Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to clear learnt values of path MTU values of IPv6 packets:

```
Router# clear ipv6 path-mtu vrf all location all
```

hw-module profile route scale ipv6-unicast connected-prefix high

To enable the IPv6 prefix scale expansion for inserting /126 and /127 IPv6 prefixes in the CEM memory instead of the LPM memory, and increase the scalability of these prefixes, use the **hw-module profile route scale ipv6-unicast connected-prefix high** command in System Admin Config mode.

Use the **no** form of the command to disable the feature.

hw-module profile route scale ipv6-unicast connected-prefix high

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default.

Command Modes

System Admin Config mode

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

The chassis must be reloaded for the **hw-module** command to be functional.

Task ID

Task ID	Operations
ipv6	read, write

```
Router# configure
Router(config)# hw-module profile route scale ipv6-unicast connected-prefix high
Tue Aug 23 18:26:42.473 UTC
In order to activate/deactivate this Route Scale IPv6-ucast connected-prefix profile, you
must manually reload the chassis/all line cards
Router(config)# commit
Tue Aug 23 18:26:57.018 UTC
Router(config)# end
```

After configuring, you must reload the router for the feature to take effect.

hw-module local-station-mac

To configure the local station MAC address for the router, use the **hw-module local-station-mac** command in the configuration mode.

hw-module **local-station-mac** *mac-address*

Syntax Description

mac-address	Specify the 12-digit local station MAC address for router.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
network	read, write
config-services	read, write

Examples

This example configures the local station MAC address for the router:

```
Router# config
Router(config)# hw-module local-station-mac B03F.C98C.B948
Router(config)# commit
```

icmp ipv4 rate-limit unreachable

To limit the rate that IPv4 Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **icmp ipv4 rate-limit unreachable** command in XR Config mode. To remove the rate limit, use the **no** form of this command.

icmp ipv4 rate-limit unreachable [**DF**] *milliseconds*
no icmp ipv4 rate-limit unreachable [**DF**] *milliseconds*

Syntax Description

DF	(Optional) Limits the rate at which ICMP destination unreachable messages are sent when code 4 fragmentation is needed and data fragmentation is (DF) set, as specified in the IP header of the ICMP destination unreachable message.
milliseconds	Time period (in milliseconds) between the sending of ICMP destination unreachable messages. Range is 1 to 4294967295.

Command Default

The default value is one ICMP destination unreachable message every 500 milliseconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The Cisco IOS XR software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **DF** option is not configured, the **icmp ipv4 rate-limit unreachable** command sets the time values for DF destination unreachable messages. If the **DF** option is configured, its time values remain independent from those of general destination unreachable messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to set the time interval for the ICMP destination unreachable message to be generated at a minimum interval of 10 ms:

```
RP/0/RP0/CPU0:router(config)# icmp ipv4 rate-limit unreachable 10
```

ipv4 address (network)

To set a primary or secondary IPv4 address for an interface, use the **ipv4 address** command in interface configuration mode. To remove an IPv4 address, use the **no** form of this command.

ipv4 address *ipv4-address mask* [**secondary**] [**route-tag** *route-tag value*]
no ipv4 address *ipv4-address mask* [**secondary**] [**route-tag** *route-tag value*]

Syntax Description

ipv4-address	IPv4 address.
mask	Mask for the associated IP subnet. The network mask can be specified in either of two ways: • The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.
secondary	(Optional) Specifies that the configured address is a secondary IPv4 address. If this keyword is omitted, the configured address is the primary IPv4 address.
route-tag	(Optional) Specifies that the configured address has a route tag to be associated with it.
route-tag value	(Optional) Value of the route tag. Range is 1 to 4294967295.

Command Default

No IPv4 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

An interface can have one primary IPv4 address and multiple secondary IPv4 addresses. Packets generated by the software always use the primary IPv4 address. Therefore, all networking devices on a segment should share the same primary network number.

Note The same IPv4 address configured on two different interfaces causes an error message to display that indicates the conflict. The interface located in the highest rack, slot, module, instance, and port is disabled.

Hosts can determine subnet masks using the IPv4 Internet Control Message Protocol (ICMP) mask request message. Networking devices respond to this request with an ICMP mask reply message.

You can disable IPv4 processing on a particular interface by removing its IPv4 address with the **no ipv4 address** command. If the software detects another host using one of its IPv4 addresses, it will display an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except that the system never generates datagrams other than routing updates with secondary source addresses. IPv4 broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IPv4 addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IPv4 addresses on the networking devices allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.

The route-tag feature attaches a tag to all IPv4 addresses. The tag is propagated from the Management Agents (MA) to the Address Repository Managers (RPM) to routing protocols, thus enabling the user to control the redistribution of connected routes by looking at the route tags via RPL scripts.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to set 192.168.1.27 as the primary address and 192.168.7.17 and 192.168.8.17 as the secondary addresses on hundredGigE interface 0/0/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.7.17 255.255.255.0 secondary
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.8.17 255.255.255.0 secondary
```

ipv4 assembler max-packets

To configure the maximum number of packets that are allowed in assembly queues, use the **ipv4 assembler max-packets** command in XR Config mode. To disable this feature, use the **no** from of this command.

ipv4 assembler max-packets *percentage value*
no ipv4 assembler max-packets *percentage value*

Syntax Description

percentage value	Percentage of total packets available in the system. The range is from 1 to 50.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to configure the maximum number of packets for the assembly queue:

```
Router(config)# ipv4 assembler max-packets 35
```

ipv4 assembler timeout

To configure the number of seconds an assembly queue can hold before a timeout occurs, use the **ipv4 assembler timeout** command in XR Config mode. To disable this feature, use the **no** form of this command.

ipv4 assembler timeout *seconds*
no ipv4 assembler timeout *seconds*

Syntax Description

seconds	Number of seconds an assembly queue can hold before a timeout occurs. The range is from 1 to 120.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to configure an assembly queue before a timeout occurs:

```
RP/0/RP0/CPU0:router(config)# ipv4 assembler timeout 88
```

ipv4 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv4 conflict-policy** command in XR Config mode. To disable the IPARM conflict resolution, use the **no** form of the command.

ipv4 conflict-policy {**highest-ip** | **longest-prefix** | **static**}
no ipv4 conflict-policy {**highest-ip** | **longest-prefix** | **static**}

Syntax Description

highest-ip	Keeps the highest ip address in the conflict set.
longest-prefix	Keeps the longest prefix match in the conflict set.
static	Keeps the existing interface running across new address configurations.

Command Default

The precedence rule adopted is loopback > physical > other virtual interfaces. Within virtual interfaces, there is an alphabetical preference, for example, loopback1 > loopback2 > tunnel. Among physical interfaces, the lower rack or slot takes control.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use **ipv4 conflict-policy** command to set an IPARM policy that resolves a conflict in the configured addresses. The policy tells IPARM what address to select from the addresses in conflict. The policy then forces the address in conflict to become inactive.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

The following example shows how to enable the static policy for conflict resolution:

```
RP/0/RP0/CPU0:router(config)# ipv4 conflict-policy static
```

ipv4 directed-broadcast

To enable forwarding of IPv4 directed broadcasts on an interface, use the **ipv4 directed-broadcast** command in interface configuration mode. To disable forwarding of IPv4 directed broadcast on an interface, use the **no** form of this command.

ipv4 directed-broadcast
no ipv4 directed-broadcast

Syntax Description

This command has no keywords or arguments.

Command Default

By default, directed broadcasts are dropped.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

A directed broadcast is a packet sent to a specific network. IPv4 directed broadcasts are dropped and not forwarded. Dropping IPv4 directed broadcasts makes routers less susceptible to denial-of-service (DoS) attacks.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to enable the forwarding of IPv4 directed broadcasts on interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface  0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv4 directed-broadcast
```

ipv4 helper-address

To configure the address to which the software forwards User Datagram Protocol (UDP) broadcasts, including BOOTP, received on an interface, use the **ipv4 helper-address** command in interface configuration mode. To remove an IPv4 helper address, use the **no** form of this command.

{**ipv4 helper-address** [**vrf** *vrf-name*][*destination-address*]}
{**no ipv4 helper-address** [**vrf** *vrf-name*][*destination-address*]}

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
destination-address	Destination broadcast or host address to be used when UDP broadcasts are forwarded. There can be more than one helper address per interface.

Command Default

IPv4 helper addresses are disabled. Default VRF is assumed if the VRF is not specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command with the **forward-protocol udp** command in mode, which specifies by port number the broadcast packets that are forwarded. UDP is enabled by default for well-known ports. The **ipv4 helper-address** command specifies the destination to which the UDP packets are forwarded.

One common application that requires IPv4 helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure an IPv4 helper address on the networking device interface physically closest to the client. The IPv4 helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one IPv4 helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the networking device. The DHCP server now receives broadcasts from the DHCP clients.

A DHCP relay profile must be configured to perform DHCP Relay. The **ip helper-address** command is used to forward broadcast UDP (non-DHCP) packets.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to specify that all UDP broadcast packets received on HundredGigEinterface 0/1/0/0 are forwarded to 192.168.1.0:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 helper-address 192.168.1.0
```

ipv4 mask-reply

To enable the software to respond to IPv4 Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ipv4 mask-reply** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipv4 mask-reply
no ipv4 mask-reply

Syntax Description

This command has no keywords or arguments.

Command Default

IPv4 mask replies are not sent.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command enables the software to respond to IPv4 ICMP mask requests by sending ICMP mask reply messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example enables the sending of ICMP mask reply messages on HundredGigEinterface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 mask-reply
```

ipv4 mtu

To set the maximum transmission unit (MTU) size of IPv4 packets sent on an interface, use the **ipv4 mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv4 mtu *bytes*
no ipv4 mtu

Syntax Description

bytes	MTU in bytes. Range is 68 to 65535 bytes for IPv4 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

Command Default

If no MTU size is configured for IPv4 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The router punts the packets that needs fragmentation; whereas the software path drops the subscriber traffic that needs fragmentation.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, if the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IPv4 MTU value. If the current IPv4 MTU value is the same as the MTU value, and you change the MTU value, the IPv4 MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IPv4 MTU value has no effect on the value for the **mtu** command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

This example shows how to set the maximum IPv4 packet size for HundredGigE interface 0/0/0/1 to 1500 bytes:

```
RP/0/(config)# interface HundredGigE0/0/0/1
RP/0/(config-if)# ipv4 mtu 1500
```

ipv4 redirects

To enable the sending of IPv4 Internet Control Message Protocol (ICMP) redirect messages if the software is forced to resend a packet through the same interface on which it was received, use the **ipv4 redirects** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipv4 redirects
no ipv4 redirects

Syntax Description

This command has no keywords or arguments.

Command Default

ICMP redirect messages are disabled by default on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

ICMP redirect messages are disabled by default on the interface.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to disable the sending of ICMP IPv4 redirect messages on &;HundredGigE interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv4 redirects
```

ipv4 source-route

To allow the processing of any IPv4 datagrams containing a source-route header option, use the **ipv4 source-route** command in XR EXEC mode. To have the software discard any IP datagram that contains a source-route option, use the **no** form of this command.

ipv4 source-route
no ipv4 source-route

Syntax Description

This command has no keywords or arguments.

Command Default

The software discards any IPv4 datagrams containing a source-route header option.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

By default, any IPv4 datagram which contains a source-route header option is discarded.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to allow the processing of any IPv4 datagrams containing a source-route header option:

```
RP/0/RP0/CPU0:router(config)# ipv4 source-route
```

ipv4 tcp-mss-adjust

To enable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv4 packets, use the **ipv4 tcp-mss-adjust** command in the interface configuration submode. To disable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU, use the **no** form of this command.

ipv4 tcp-mss-adjust enable
no ipv4 tcp-mss-adjust enable

Syntax Description

enable	Enables Maximum Segment Size (MSS) adjustment for tcp flows on the interface.

Command Default

None

Command Modes

Interface Configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
mpls-te	read, write
ipv4	read, write
network	read, write
acl	read, write

Example

This example shows how to enable the transit traffic of TCP flows for IPv4 packets using the **ipv4 tcp-mss-adjust** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/0/0/4.20
RP/0/RP0/CPU0:router(config-if)# ipv4 tcp-mss-adjust enable
```

Related Commands

Command	Description
ipv6 tcp-mss-adjust, on page 415	Enables the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv6 packets.

ipv4 unnumbered (point-to-point)

To enable IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface, use the **ipv4 unnumbered** command in an interface configuration mode. To disable this feature, use the **no** form of this command.

ipv4 unnumbered *interface-type interface-instance*
no ipv4 unnumbered *interface-type interface-instance*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-instance	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

IPv4 processing on a point-to-point interface is disabled unless an IPv4 address is assigned explicitly to that interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

For release Release 4.2.0 onward, to enter the dynamic template configuration mode, run the **dynamic-template** command in the XR Config mode.

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IPv4 packet. It also uses the IPv4 address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.

The interface you specify by the *interface-type* and *interface-number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

This example shows how the HundredGigE interface 0/0/0/1 is assigned the loopback interface address 5:

```
RP/0/RP0/CPU0:router(config)# interface loopback 5
RP/0/RP0/CPU0:router(config-if)# ipv4 address 192.168.6.6 255.255.255.0
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5
```

ipv4 unreachables disable

To disable the generation of IPv4 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv4 unreachables disable** command in an interface configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv4 unreachables disable
no ipv4 unreachables disable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv4 ICMP unreachables messages are generated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP protocol unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects a number of ICMP unreachable messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

Examples

This example shows how to disable the generation of ICMP unreachable messages on HundredGigE interface 0/0/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 unreachables disable
```

ipv4 virtual address

To define an IPv4 virtual address for a network of management Ethernet interfaces, use the **ipv4 virtual interface** command in XR Config mode. To remove an IPv4 virtual address from the configuration, use the **no** form of this command.

ipv4 virtual address {[**vrf** *vrf-name*] *ipv4-address*/*mask* | **use-as-src-addr**}
no ipv4 virtual address {[**vrf** *vrf-name*] *ipv4-address*/*mask* | **use-as-src-addr**}

Syntax Description

vrf *vrf-name*	(Optional) Configures the virtual address on a per VPN routing and forwarding (VRF) basis for the management interfaces The *vrf-name* argument specifies the name of the VRF.
ipv4 address	Virtual IPv4 address and the mask that is to be unconfigured.
mask	Mask for the associated IP subnet. The network mask can be specified in either of two ways: • The network mask can be a four-part dotted-decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address. A slash between numbers is required as part of the notation.
use-as-src-addr	Enables the virtual address to be used as the default SRC address on sourced packets.

Command Default

No IPv4 virtual address is defined for the configuration.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2	This release supports virtual addresses for the hosted Linux networking stack.
Release 7.0.12	This command was introduced.

Usage Guidelines

Configuring an IPv4 virtual address enables you to access the router from a single virtual address with a management network. An IPv4 virtual address persists across route processor (RP) failover situations.

Configuring an IPv4 virtual address enables you to access a dual RP router from a single address without prior knowledge of which RP is active. An IPv4 virtual address persists across RP failovers. For this to happen, the virtual IPv4 address must share a common IPv4 subnet with a Management Ethernet interface on both RPs.

If you disable the **ipv4 virtual address** command with the **vrf** keyword, the virtual IP address is unconfigured for the corresponding VRF or for the default if no VRF is specified. This results in the removal of the entry for the virtual IP address in the VRF table and in the ARP cache.

The default VRF is chosen when no VRF is specified. The virtual IP address is activated on a management interface that is attached to a default VRF.

The **use-as-src-addr** keyword eliminates the need for configuring a loopback interface as the source interface (that is, update source) for management applications. When an update source is not configured, management applications allow the transport processes (TCP, UDP, raw_ip) to pick a suitable source address. The transport processes, in turn, consult the FIB to do so. If a Management Ethernet's IP address is picked as the source address and if the **use-as-src-addr keyword** is configured, then the transport processes replace the Management Ethernet's IP address with a relevant virtual IP address. This functionality works across RP switchovers.

Cisco IOS XR Software Release 7.5.2 and later also supports virtual addresses for the hosted Linux networking stack.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to define an IPv4 virtual address:

```
Router(config)# ipv4 virtual address 10.3.32.154/8
```

The following example show how to configure the virtual IP addresses for management interfaces on a per VRF basis:

```
Router(config)# ipv4 virtual address vrf ppp 10.26.3.4/16
```

ipv6 address

To configure an IPv6 address for an interface and enable IPv6 processing on the interface using an EUI-64 interface ID in the low-order 64 bits of the address, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix/prefix-length* [**eui-64**] [**route-tag** *route-tag value*]
no ipv6 address *ipv6-prefix/prefix-length* [**eui-64**] [**route-tag** *route-tag value*]

Syntax Description

ipv6-prefix	The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
eui-64	(Optional) Specifies an interface ID in the low-order 64 bits of the IPv6 address.
route-tag	(Optional) Specifies that the configured address has a route tag to be associated with it.
route-tag value	(Optional) Value of the route tag. Range is 1 to 4294967295.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If the value specified for the / *prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS XR software detects another host using one of its IPv6 addresses, it displays an error message on the console.

The route-tag feature attaches a tag to all IPv6 addresses. The tag is propagated from the Management Agents (MA) to the Address Repository Managers (RPM) to routing protocols, thus enabling the user to control the redistribution of connected routes by looking at the route tags via RPL scripts.

Task ID

Task ID	Operations
ipv6	read, write

Task ID	Operations
network	read, write

Examples

The following example assigns IPv6 address 2001:0DB8:0:1::/64 to HundredGigE interface 0/0/0/1 and specifies an EUI-64 interface ID in the low-order 64 bits of the address:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

ipv6 address link-local

To configure an IPv6 link-local address for an interface and enable IPv6 processing on the interface, use the **ipv6 address link-local** command in interface configuration mode. The *ipv6-address* value specified with this command overrides the link-local address that is automatically generated for the interface. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address* **link-local** [**route-tag** *route-tag value*]
no ipv6 address *ipv6-address* **link-local** [**route-tag** *route-tag value*]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-local	Specifies a link-local address. The *ipv6-address* value specified with this command overrides the link-local address that is automatically generated for the interface.
route-tag	(Optional) Specifies that the configured address has a route-tag to be associated with it.
route-tag value	(Optional) Displays the route-tag value. Range is 1 to 4294967295.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If the Cisco IOS XR software detects another host using one of its IPv6 addresses, the software displays an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 address link-local** command.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to assign FE80::260:3EFF:FE11:6770 as the link-local address for HundredGigE interface 0/0/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

ipv6 assembler

To configure the maximum number of packets that are allowed in assembly queues or to configure the number of seconds an assembly queue will hold before timeout , use the **ipv6 assembler** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

ipv6 assembler {**max-packets** *value* | **timeout** *seconds*}
no ipv6 assembler {**max-packets** *value* | **timeout** *seconds*}

Syntax Description

max-packets	Maximum packets allowed in assembly queues.
timeout	Number of seconds an assembly queue will hold before timeout.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ipv6	read, write

Example

The following example shows how to configure the maximum number of packets that are allowed in assembly queues:

```
Router# config
Router(config)# ipv6 assembler max-packets 35
```

ipv6 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv6 conflict-policy** command in XR Config mode mode. To disable the IPARM conflict resolution, use the **no** form of the command.

ipv6 conflict-policy {**highest-ip** | **longest-prefix** | **static**}
no ipv6 conflict-policy {**highest-ip** | **longest-prefix** | **static**}

Syntax Description

highest-ip	Keeps the highest IP address in the conflict set.
longest-prefix	Keeps the longest prefix match in the conflict set.
static	Keeps the existing interface running across new address configurations.

Command Default

Default is the lowest rack/slot if no conflict policy is configured.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read, write
ip-services	read, write

Examples

The following example shows how to enable the longest prefix policy for conflict resolution:

```
RP/0/RP0/CPU0:router(config)# ipv6 conflict-policy longest-prefix
```

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in an appropriate configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

None

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR EXEC mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to enable IPv6 processing on HundredGigE interface 0/0/0/1:

```
Router(config)# interface HundredGigE0/0/0/1
Router(config-if)# ipv6 enable
```

ipv6 hop-limit

To configure the maximum number of hops used in router advertisements and all IPv6 packets that are originated by the router, use the **ipv6 hop-limit** command in XR Config mode mode. To return the hop limit to its default value, use the **no** form of this command.

ipv6 hop-limit *hops*
no ipv6 hop-limit *hops*

Syntax Description

hops	Maximum number of hops. Range is 1 to 255.

Command Default

hops : 64 hops

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to configure a maximum number of 15 hops for router advertisements and all IPv6 packets that are originated from the router:

```
RP/0/RP0/CPU0:router(config)# ipv6 hop-limit 15
```

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages on all nodes, use the **ipv6 icmp error-interval** command in XR Config mode mode. To return the interval to its default setting, use the **no** form of this command.

ipv6 icmp error-interval *milliseconds* [*bucketsize*]
no ipv6 icmp error-interval

Syntax Description

milliseconds	Time interval (in milliseconds) between tokens being placed in the bucket. Range is 0 to 2147483647.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is 1 to 200 with a default of 10 tokens.

Command Default

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero.

milliseconds : 100 milliseconds

bucketsize : 10 tokens

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **ipv6 icmp error-interval** command in XR Config mode mode to limit the rate at which IPv6 ICMP error messages are sent for each node. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens being placed in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens stored in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* argument is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Use the **show ipv6 traffic** EXEC command to display IPv6 ICMP rate-limited counters.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
RP/0/RP0/CPU0:router(config)# ipv6 icmp error-interval 50 20
```

ipv6 mtu

To set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface, use the **ipv6 mtu** command in an appropriate configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*
no ipv6 mtu

Syntax Description

bytes	MTU in bytes. Range is 1280 to 65535 for IPv6 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

Command Default

If no MTU size is configured for IPv6 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If an IPv6 packet exceeds the MTU set for the interface, only the source router of the packet can fragment it.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, If the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IPv6 MTU value. If the current IPv6 MTU value is the same as the MTU value, and you change the MTU value, the IPv6 MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IPv6 MTU value has no effect on the value for the **mtu** command.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Task ID	Operations
config-services	read, write

Examples

This example (not applicable for BNG) shows how to set the maximum IPv6 packet size for HundredGigE interface 0/0/0/1 to 1350 bytes:

```
Router(config)# interface HundredGigE0/0/0/1
Roputer(config-if)# ipv6 mtu 1350
```

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface, use the **ipv6 nd dad attempts** command in an appropriate configuration mode. To return the number of messages to the default value, use the **no** form of this command.

ipv6 nd dad attempts *value*
no ipv6 nd dad attempts *value*

Syntax Description

value	Number of neighbor solicitation messages. Range is 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Command Default

Duplicate address detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled. The default is one message.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 2462, *IPv6 Stateless Address Autoconfiguration*) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on a tentative unicast IPv6 address.

The interval between the sending of duplicate address detection neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 2461, *Neighbor Discovery for IP Version 6 [IPv6]*), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when the address is being resolved or when the reachability of a neighbor is being probed. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the **ipv6 nd ns-interval** command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the .

Note An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to duplicate and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
ipv6_nd[145]: %IPV6_ND-3-ADDRESS_DUPLICATE : Duplicate address 111::1 has been detected
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%IPV6-4-DUPLICATE: Duplicate address 3000::4 on &HundredGigE;
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to duplicate.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Task ID

Task ID	Operations
ipv6	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to set the number of consecutive neighbor solicitation messages for interface 0/2/0/1 to 1 and then display the state (tentative or duplicate) of the unicast IPv6 address configured for an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/2/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd dad attempts 1
RP/0/RP0/CPU0:router(config-if)# Uncommitted changes found, commit them before
exiting(yes/no/cancel)? [cancel]:y

RP/0/RP0/CPU0:router# show ipv6 interface
HundredGigE/2/0/0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
HundredGigE/2/0/1 is Up, line protocol is Up
  IPv6 is enabled, link-local address is fe80::203:fdff:fe1b:4501
  Global unicast address(es):
    1:4::1, subnet is 1:4::/64 [DUPLICATE]
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
HundredGigE/2/0/2 is Shutdown, line protocol is Down
  IPv6 is enabled, link-local address is fe80::200:11ff:fe11:1111 [TENTATIVE]
  Global unicast address(es):
    111::2, subnet is 111::/64 [TENTATIVE]
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

For BNG, this example shows how to display the state (tentative or duplicate) of the unicast IPv6 address on the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd dad attempts 1
```

ipv6 nd managed-config-flag

To set the managed address configuration flag in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The managed address configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Setting the managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR EXEC mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to configure the managed address configuration flag in IPv6 router advertisements on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd managed-config-flag
```

For BNG, this example shows how to configure the managed address configuration flag in IPv6 router advertisements on dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in an appropriate configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

Syntax Description

milliseconds	Interval (in milliseconds) between IPv6 neighbor solicit transmissions. Range is 1000 to 3600000.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements, and the value 1000 is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This value is included in all IPv6 router advertisements sent out from this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ns-interval 9000
```

For BNG, this example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ns-interval 9000
```

ipv6 nd other-config-flag

To set the other stateful configuration flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note If the managed address configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the other stateful configuration flag.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd other-config-flag
```

For BNG, this example configures the “other stateful configuration” flag for IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd other-config-flag
```

ipv6 nd prefix

To configure how IPv6 prefixes are advertised in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To advertise a prefix with default parameter values, use the **no** form of this command. To prevent a prefix (or prefixes) from being advertised, use the **no- adv** keyword.

ipv6 nd prefix {*ipv6prefix/prefix-length* | **default** [*valid-lifetime* | **at** | **infinite** | **no-adv** | **no-autoconfig** | **off-link**]}
no ipv6 nd prefix {*ipv6prefix/prefix-length* | **default** [*valid-lifetime* | **at** | **infinite** | **no-adv** | **no-autoconfig** | **off-link**]}

Syntax Description

ipv6-prefix	The IPv6 network number to include in router advertisements. This keyword must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
default	(Optional) Specifies all prefixes.
valid-lifetime	(Optional) The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. The range of values is 0 to 4294967295 seconds.
at	(Optional) The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire.*
infinite	(Optional) The valid lifetime does not expire.
no-adv	(Optional) The prefix is not advertised.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. This prefix should not be used for *onlink* determination.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

To control how prefixes are advertised, use the **ipv6 nd prefix** command. By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised with default values. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, only the specified prefixes are advertised with the configured values, all other prefixes are advertised with default values.

The default keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix is no longer advertised.

When onlink is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out HundredGigE interface 0/1/0/0 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

ipv6 nd ra dns server

To configure the IPv6 router advertisement of DNS server addresses on an interface, use the **ipv6 nd ra dns server** command in interface configuration mode. To remove the IPv6 router advertisement of DNS server addresses, use the **no** form of this command.

ipv6 nd ra dns server *ipv6-address* {*seconds* | **infinite-lifetime** | **zero-lifetime** }
no ipv6 nd ra dns server *ipv6-address*
no ipv6 nd ra dns server

Syntax Description

server *ipv6-address*	Specify the DNS server address to be advertised in an IPv6 router advertisement (RA).
seconds | **infinite-lifetime** | **zero-lifetime**	The amount of time that the DNS server is advertised in an IPv6 RA. The range for seconds is from 200 to 4294967295. The lifetime can also be specified as infinite or zero.

Command Default

The DNS server is not advertised in an IPv6 RA.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This configuration is not allowed for management interfaces.

You can use the **ipv6 nd ra dns server** command to configure up to five DNS server addresses in an RA.

If you configure a seconds value of zero, the DNS server will no longer be used.

Use the **no ipv6 nd ra dns server** *ipv6-address* command to delete a single DNS server under an interface. Use the **no ipv6 nd ra dns server** command to delete all DNS servers under an interface.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

The following example configures a DNS server with an IPv6 address of 2001:DB8:1::1 to be advertised in an RA with a lifetime of 600 seconds:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/2/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra dns server 2001:DB8:1::1 600
```

The following example configures a DNS server with an IPv6 address of 4::4 to be advertised in an RA with an infinite lifetime:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/2/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra dns server 4::4 infinite-lifetime
```

Related Commands

Command	Description
ipv6 nd ra-lifetime, on page 400	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface , on page 441	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra dns search list

To configure the IPv6 router advertisement of DNS search list on an interface, use the **ipv6 nd ra dns search list** command in interface configuration mode. To remove the IPv6 router advertisement of DNS search list, use the **no** form of this command.

ipv6 nd ra dns search list *name* {*seconds* | **infinite-lifetime** | **zero-lifetime** }
no ipv6 nd ra dns search list *name*
no ipv6 nd ra dns search list

Syntax Description

name	Specify the DNS search list to be advertised in an IPv6 router advertisement (RA).
seconds | **infinite-lifetime** | **zero-lifetime**	The amount of time that the DNS search list is advertised in an IPv6 RA. The range for seconds is from 200 to 4294967295. The lifetime can also be specified as infinite or zero.

Command Default

The DNS search list is not advertised in an IPv6 RA.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This configuration is not allowed for management interfaces.

You can use the **ipv6 nd ra dns search list** command to configure up to 50 DNS search lists in an RA.

If you configure a seconds value of zero, the DNS server will no longer be used.

Use the **no ipv6 nd ra dns search list** *name* command to delete a single DNS search list under an interface. Use the **no ipv6 nd ra dns search list** command to delete all DNS search lists under an interface.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

The following example configures a DNS search list with a name of aaa.cc.com to be advertised in an RA with an infinite lifetime:

```
Router(config)# interface GigabitEthernet 0/2/0/0
Router(config-if)# ipv6 nd ra dns search list aaa.cc.com infinite-lifetime
```

Related Commands

Command	Description
ipv6 nd ra-lifetime, on page 400	Configures the lifetime of an IPv6 router advertisement.
ipv6 nd ra-lifetime, on page 400	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in an appropriate configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval *seconds*
no ipv6 nd ra-interval *seconds*

Syntax Description

seconds	The interval (in seconds) between IPv6 router advertisement transmissions.

Command Default

seconds : 200 seconds

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the router is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures an IPv6 router advertisement interval of 201 seconds on HundredGigE interface 0/1/0/1:

```
Router(config)# interface HundredGigE0/1/0/1
Router(config-if)# ipv6 nd ra-interval 201
```

For BNG, this example configures an IPv6 router advertisement interval of 201 seconds in the dynamic template configuration mode:

```
Router(config)# dynamic-template type ppp p1
Router(config-dynamic-template-type)# ipv6 nd ra-interval 201
```

ipv6 nd ra-lifetime

To configure the router lifetime value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in an appropriate configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*
no ipv6 nd ra-lifetime

Syntax Description

seconds	The validity (in seconds) of this router as a default router on this interface.

Command Default

seconds : 1800 seconds

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Usage Guidelines

The router lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The router lifetime value can be set to a nonzero value to indicate that it should be considered a default router on this interface. The nonzero value for the router lifetime value should not be less than the router advertisement interval.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) configures an IPv6 router advertisement lifetime of 1801 seconds on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra-lifetime 1801
```

For BNG, this example configures an IPv6 router advertisement lifetime of 1801 seconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd ra-lifetime 1801
```

ipv6 nd ra specific route

To configure specific route for a router on a specific interface, use the **ipv6 nd ra specific route** command in interface configuration mode. To delete a single or all specific routes, use the **no** form of this command.

ipv6 nd ra specific route *prefix* **Lifetime** {*seconds* | **infinite-lifetime** | **zero-lifetime** }**[preference** { **high** | **medium** | **low** }**]**
no ipv6 nd ra specific route *prefix*
no ipv6 nd ra specific route

Syntax Description

route *prefix*	Variable-length field containing an IP address or a prefix of an IP address to identify a route.
Lifetime {*seconds* | **infinite-lifetime** | **zero-lifetime**}	The length of time the route prefix is valid for route determination specified as seconds, infinite, or zero.
[preference {**high** | **medium** | **low** }**]**	(Optional) Preference for the router specified on an interface specified as high, medium, or low.

Command Default

Router advertisements (RAs) are sent with the medium preference.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This configuration is not allowed for management interfaces.

If the Lifetime is set to zero, then the host will no longer use the router for route aspect of the route information option.

If no preference is specified, then the default value for preference (medium) is used.

Use the **no ipv6 nd ra specific route** *prefix* command to delete a single specific route under an interface. Use the **no ipv6 nd ra specific route** command to delete all specific routes under an interface.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

The following example configures a specific route for the router on gigabit Ethernet interface 0/2/0/0:

```
Router(config)# interface GigabitEthernet 0/2/0/0
Router(config-if)# ipv6 nd ra specific route 3::3/116 Lifetime 1112 preference low
```

Related Commands

Command	Description
ipv6 nd ra-lifetime, on page 400	Configures the lifetime of an IPv6 router advertisement.
ipv6 nd ra-lifetime, on page 400	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in an appropriate configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *milliseconds*
no ipv6 nd reachable-time

Syntax Description

milliseconds	The amount of time (in milliseconds) that a remote IPv6 node is considered reachable. The range is from 0 to 3600000.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements and 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 indicates that the configured time is unspecified by this router.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to configure an IPv6 reachable time of 1,700,000 milliseconds for HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-if)# ipv6 nd reachable-time 1700000
```

For BNG, this example shows how to configure an IPv6 reachable time of 1,700,000 milliseconds in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd reachable-time 1700000
```

ipv6 nd redirects

To send Internet Control Message Protocol (ICMP) redirect messages, use the **ipv6 nd redirects** command in interface configuration mode. To restore the system default, use the **no** form of this command.

ipv6 nd redirects
no ipv6 nd redirects

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to redirect IPv6 nd-directed broadcasts on HundredGigE interface 0/2/0/2:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 nd redirects
```

ipv6 nd router-preference

To configure a default router preference (DRP) for the router on a specific interface, use the **ipv6 nd router-preference** command in interface configuration mode. To return to the default DRP, use the **no** form of this command.

ipv6 nd router-preference {**high** | **medium** | **low** }
no ipv6 nd router-preference

Syntax Description

high	Preference for the router specified on an interface is high.
medium	Preference for the router specified on an interface is medium.
low	Preference for the router specified on an interface is low.

Command Default

Router advertisements (RAs) are sent with the medium preference.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This configuration is not allowed for management interfaces.

RA messages are sent with the DRP configured by the ipv6 nd router-preference command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

The following example configures a DRP of high for the router on gigabit Ethernet interface 0/2/0/0:

```
Router(config)# interface GigabitEthernet 0/2/0/0
Router(config-if)# ipv6 nd router-preference high
```

Related Commands

Command	Description
ipv6 nd ra-lifetime, on page 400	Configures the lifetime of an IPv6 router advertisement.
ipv6 nd ra-lifetime, on page 400	Displays the usability status of interfaces configured for IPv6.

ipv6 nd scavenge-timeout

To set the lifetime for neighbor entries in the stale state, use the **ipv6 nd scavenge-timeout** command in XR Config mode mode. To disable this feature, use the **no** form of this command.

ipv6 nd scavenge-timeout *seconds*
no ipv6 nd scavenge-timeout *seconds*

Syntax Description

seconds	RA lifetime in seconds. The range is from 0 to 43200.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When the scavenge-timer for a neighbor entry expires, the entry is cleared.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to set the lifetime for the neighbor entry:

```
RP/0/RP0/CPU0:router(config)# ipv6 nd scavenge-timeout 3000
```

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in an appropriate configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 router advertisements are automatically sent on other types of interlaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR Config mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to suppress IPv6 router advertisements on HundredGigE interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv6 nd suppress-ra
```

For BNG, this example shows how to suppress IPv6 router advertisements in the dynamic template configuration mode:

```
RP/0/RP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RP0/CPU0:router(config-dynamic-template-type)# ipv6 nd suppress-ra
```

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in XR Config mode mode. To remove a static IPv6 entry from the IPv6 neighbors discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*
no ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*

Syntax Description

ipv6-address	The IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-instance	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
hardware-address	The local data-link address (a 48-bit address).

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

Use the **show ipv6 neighbors** command to display static entries in the IPv6 neighbors discovery cache. A static entry in the IPv6 neighbor discovery cache has one state: reach (reachable)—The interface for this entry is up. If the interface for the entry is down, the **show ipv6 neighbors** command does not show the entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the reach (reachable) state are different for dynamic and static cache entries. See the **show ipv6 neighbors** command for a description of the reach (reachable) state for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbors discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to reach [reachable]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Note Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to configure a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on ethernet interface 0/RSP0/CPU0:

```
RP/0/RP0/CPU0:router(config)# ipv6 neighbor 2001:0DB8::45A 0002.7D1A.9472
```

ipv6 path-mtu enable

To enable the command to configure path maximum transmission unit (MTU) discovery of IPv6 packets, use the **ipv6 path-mtu enable** command in the XR Config mode.

ipv6 path-mtu enable

Command Default

None.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to enable path MTU discovery command of IPv6 packets:

```
RP/0/RP0/CPU0:router(config)#  ipv6 path-mtu enable
```

ipv6 path-mtu timeout

To set the maximum transmission unit (MTU) timeout value of IPv6 packets, use the **ipv6 path-mtu timeout** command in the XR Config mode.

ipv6 path-mtu timeout *minutes*

Syntax Description

minutes	MTU timeout in minutes. Range is 1 to 15 minutes. Default timeout value is 10 minutes.

Command Default

None.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to set path MTU timeout of IPv6 packets:

```
RP/0/RP0/CPU0:router(config)#  ipv6 path-mtu timeout 15
```

ipv6 source-route

To enable processing of the IPv6 type source (type 0) routing header, use the **ipv6 source-route** command in XR EXEC mode mode. To disable the processing of this IPv6 extension header, use the **no** form of this command.

ipv6 source-route
no ipv6 source-route

Syntax Description

This command has no keywords or arguments.

Command Default

The **no** version of the **ipv6 source-route** command is the default.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **no ipv6 source-route** command (which is the default) prevents hosts from performing source routing using your routers. When the **no ipv6 source-route** command is configured and the router receives a packet with a type 0 source routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.

Task ID

Task ID	Operation
network	read, write
ipv6	read, write

Example

The following example shows how to allow the processing of any IPv6 datagrams containing a source-route header option:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# ipv6 source-route
RP/0/RP0/CPU0:router(config)#
```

ipv6 tcp-mss-adjust

To enable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU so that traffic fragmentation is prevented when a session is established for IPv6 packets, use the **ipv6 tcp-mss-adjust** command in the interface configuration submode. To disable the transit traffic of TCP flows to be a Maximum Segment Size (MSS) below the GRE tunnel interface or VLAN sub-interface MTU, use the **no** form of this command.

ipv6 tcp-mss-adjust enable
no ipv6 tcp-mss-adjust enable

Syntax Description

enable	Enables Maximum Segment Size (MSS) adjustment for tcp flows on the interface..

Command Default

None

Command Modes

Interface Configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This command has no keywords or arguments.

Task ID

Task ID	Operation
mpls-te	read, write
ipv6	read, write

Example

This example shows how to enable the transit traffic of TCP flows for IPv6 packets using the **ipv6 tcp-mss-adjust** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface HundredEthernet 0/0/0/4.20
RP/0/RP0/CPU0:router(config-if)# ipv6 tcp-mss-adjust enable
```

ipv6 unreachables disable

To disable the generation of IPv6 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv6 unreachables disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv6 unreachables disable
no ipv6 unreachables disable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 ICMP unreachables messages are generated.

Command Modes

Interface configuration (not applicable for BNG)

Dynamic template configuration (for BNG)

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP protocol unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects a number of ICMP unreachable messages.

For BNG, ensure you run this command in the dynamic template configuration mode. To enter the dynamic template configuration mode, run **dynamic-template** command in the XR EXEC mode.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example (not applicable for BNG) shows how to disable the generation of ICMP unreachable messages on HundredGigE interface 0/6/0/0:

```
Router(config)# interface HundredGigE0/6/0/0
Router(config-if)# ipv6 unreachables disable
```

ipv6 virtual address

To define an IPv6 virtual address for a network of management Ethernet interfaces, use the **ipv6 virtual address** command in XR Config mode. To remove an IPv6 virtual address from the configuration, use the **no** form of this command.

ipv6 virtual address {**vrf** *vrf-nameipv6-address/prefix-length* | **use-as-src-addr**}
no ipv6 virtual address {[**vrf** *vrf-name*]*ipv6-address/prefix-length* | **use-as-src-addr**}

Syntax Description

vrf *vrf-name*	(Optional) Configures the virtual address on a per VPN routing and forwarding (VRF) basis for the management interfaces The *vrf-name* argument specifies the name of the VRF.
ipv6 address	The virtual IPv6 address to be used.
prefix-length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
use-as-src-addr	Enables the virtual address to be used as the default SRC address on sourced packets.

Command Default

No IPv6 virtual address is defined for the configuration.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2	This release supports virtual addresses for the hosted Linux networking stack.
Release 7.0.12	This command was introduced.

Usage Guidelines

Configuring an IPv6 virtual address enables you to access the router from a single virtual address with a management network. An IPv6 virtual address persists across route processor (RP) failover situations.

Configuring an IPv6 virtual address enables you to access a dual RP router from a single address without prior knowledge of which RP is active. An IPv6 virtual address persists across RP failovers. For this to happen, the virtual IPv6 address must share a common IPv6 subnet with a Management Ethernet interface on both RPs.

If you disable the **ipv6 virtual address** command with the **vrf** keyword, the virtual IP address is unconfigured for the corresponding VRF or for the default if no VRF is specified. This results in the removal of the entry for the virtual IP address in the VRF table and in the ARP cache.

The default VRF is chosen when no VRF is specified. The virtual IP address is activated on a management interface that is attached to a default VRF.

The **use-as-src-addr** keyword eliminates the need for configuring a loopback interface as the source interface (that is, update source) for management applications. When an update source is not configured, management applications allow the transport processes (TCP, UDP, raw_ip) to pick a suitable source address. The transport processes, in turn, consult the FIB to do so. If a Management Ethernet's IP address is picked as the source address and if the **use-as-src-addr keyword** is configured, then the transport processes replace the Management Ethernet's IP address with a relevant virtual IP address. This functionality works across RP switchovers.

Cisco IOS XR Software Release 7.5.2 and later also supports virtual addresses for the hosted Linux networking stack.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to define an IPv6 virtual address:

```
RP/0/RP0/CPU0:router(config)# ipv6 virtual address 0:0:0:7272::72/64
```

The following example shows how to configure the virtual IP addresses for management interfaces on a per VRF basis:

```
RP/0/RP0/CPU0:router(config)# ipv6 virtual address vrf ppp 0:0:0:7272::72/64
```

local pool

To create one or more local address pools from which IP addresses are assigned when a peer connects, use the **local pool** command in XR Config mode. To restore the default behavior, use the **no** form of this command.

local pool [**ipv4**] [**vrf** *vrf_name*] {*poolname* | **default**} *first-ip-address* [*last-ip-address*]
no local pool [**ipv4**] [**vrf** *vrf_name*] {*poolname* | **default**} *first-ip-address* [*last-ip-address*]

Syntax Description

vrf	Specifies that a VRF name will be given. If is parameter is missing, the default VRF is assumed.
vrf_name	Specifies the name of the VRF to which the addresses of the pool belongs. If no name is given, the default VRF is assumed.
default	Creates a default local IPv4 address pool that is used if no other pool is named.
poolname	Specifies the name of the local IPv4 address pool.
first-ip-address	Specifies the first address in an IPv4 address range. If high-IP-address is not specified, the address range is considered to have only one address.
last-ip-address	(Optional) Specifies the last address in an IPv4 address range. If high-IP-address is not specified, the address range is considered to have only one address.

Command Default

Special default pool if VRF is not specified. By default, this functionality is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to create local address pools to use in assigning IP addresses when a peer connects. You can also add range of IP addresses to an existing pool. If no pool name is specified, the pool with the name "default" is used.

The optional **vrf** keyword and associated *vrf name* allows the association of an IPv4 address pool with a named VRF. Any IPv4 address pool created without the **vrf** keyword automatically becomes a member of a default VRF. An IPv4 address pool name can be associated with only one VRF. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IPv4 address pool name with a different VRF is rejected. Therefore, each use of a pool name is an implicit selection of the associated VRF.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the default pool only in the default VRF.

All IPv4 address pools within a VRF are checked to prevent overlapping addresses; however, addresses may overlap across different VRFs.

Task ID

Task ID	Operations
ipv4	read, write
ipv6	read, write
network	read, write

Examples

The following example creates a local IPv4 address pool named “pool2,” which contains all IPv4 addresses in the range 172.16.23.0 to 172.16.23.255:

```
RP/0/RP0/CPU0:router(config)# local pool ipv4 pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
RP/0/RP0/CPU0:router(config)#no local pool ipv4 default
RP/0/RP0/CPU0:router(config)#local pool ipv4 default 10.1.1.0 10.1.4.255
```

Note It is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IPv4 addresses. To extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IPv4 addresses into one pool:

```
RP/0/RP0/CPU0:router(config)#local pool ipv4 default 10.1.1.0 10.1.9.255
RP/0/RP0/CPU0:router(config)#local pool ipv4 default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IPv4 address pools in the base system group:

```
RP/0/RP0/CPU0:router(config)#local pool vrf grp1 ipv4 p1_g1 10.1.1.1 10.1.1.50
RP/0/RP0/CPU0:router(config)#local pool vrf grp1 ipv4 p2_g1 10.1.1.100 10.1.1.110
RP/0/RP0/CPU0:router(config)#local pool vrf grp2 ipv4 p1_g2 10.1.1.1 10.1.1.40
RP/0/RP0/CPU0:router(config)#local pool ipv4 lp1 10.1.1.1 10.1.1.10
RP/0/RP0/CPU0:router(config)#local pool vrf grp1 ipv4 p3_g1 10.1.2.1 10.1.2.30
RP/0/RP0/CPU0:router(config)#local pool vrf grp2 ipv4 p2_g2 10.1.1.50 10.1.1.70
RP/0/RP0/CPU0:router(config)#local pool ipv4 lp2 10.1.2.1 10.1.2.10
```

In this example:

- VRF grp1 consists of pools p1_g1, p2_g1, and p3_g1.
- VRF grp2 consists of pools p1_g2 and p2_g2.
- Pools lp1 and lp2 are not explicitly associated with a vrf and are therefore members of the default vrf.

Note IPv4 address 10.1.1.1 overlaps in vrfs grp1, grp2 and the default vrf . There is no overlap within any vrf that includes the default vrf.

The following examples shows the configurations of IP address pools and groups for use by a VPN and VRF:

```
RP/0/RP0/CPU0:router(config)# local pool vrf vpn1 ipv4 p1_vpn1 10.1.1.1 10.1.1.50
RP/0/RP0/CPU0:router(config)# local pool vrf vpn1 ipv4 p2_vpn1 10.1.1.100 10.1.1.110
RP/0/RP0/CPU0:router(config)# local pool vrf vpn2 ipv4 p1_vpn2 10.1.1.1 10.1.1.40
RP/0/RP0/CPU0:router(config)# local pool ipv4 lp1 10.1.1.1 10.1.1.10
RP/0/RP0/CPU0:router(config)# local pool vrf vpn1 ipv4 p3_vpn1 10.1.2.1 10.1.2.30
RP/0/RP0/CPU0:router(config)# local pool vrf vpn2 ipv4 p2_vpn2 10.1.1.50 10.1.1.70 group
vpn2
RP/0/RP0/CPU0:router(config)# local pool ipv4 lp2 10.1.2.1 10.1.2.10
```

These examples show configuration of pools in two VRFs and the default VRF:

- VRF vpn1 consists of pools p1_vpn1, p2_vpn1, and p3_vpn1.
- VRF vpn2 consists of pools p1_vpn2 and p2_vpn2.
- Pools lp1 and lp2 are not associated with a VRF and therefore belong to the default VRF.

Note IPv4 address 10.1.1.1 overlaps across VRFs vpn1, vpn2 and the default VRF . There is no overlap within any VRF.

The VPN requires a configuration that selects the proper vrf by selecting the proper pool based on remote user data. Each user in a given VPN can select an address space using the pool and associated vrf appropriate for that VPN. Duplicate addresses in other VPNs (other vrfs) are not a concern, because the address space of a VPN is specific to that VPN. In the example, a user in VRF vpn1 is associated with a combination of the pools p1_vpn1, p2_vpn1, and p3_vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

show arm conflicts

To display IPv4 or IPv6 address conflict information identified by the Address Repository Manager (ARM), use the **show arm conflicts** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} [**vrf** *vrf-name*] **conflicts** [**address** | **override** | **unnumbered**]

Syntax Description

ipv4	Displays IPv4 address conflicts.
ipv6	Displays IPv6 address conflicts.
vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information. Available for IPv4 only.
vrf-name	(Optional) Name of a VRF.
address	(Optional) Displays address conflict information.
override	(Optional) Displays address conflict override information.
unnumbered	(Optional) Displays unnumbered interface conflict information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show arm conflicts** command to display information about IPv4 or IPv6 address conflicts. You can use address conflict information to identify misconfigured IPv4 or IPv6 addresses.

Conflict information is displayed for interfaces that are forced down and for interfaces that are up.

Issuing the **show arm conflicts** command without specifying any optional keywords displays the output generated from both the **address** and **unnumbered** keywords.

Task ID

Task ID	Operations
network	read

Examples

The following sample output is from the **show arm ipv4 conflicts** command:

```
RP/0/RP0/CPU0:router# show arm ipv4 conflicts

F Forced down
| Down interface & addr                  Up interface & addr

F Lo2 10.1.1.2/24                         Lo1 10.1.1.1/24
```

```
Forced down interface          Up interface
tu2->tu1                       tu1->Lo1
```

The following is sample output from the **show arm ipv4 conflicts** command with the **address** keyword:

```
RP/0/RP0/CPU0:router# show arm ipv4 conflicts address

F Forced down
| Down interface & addr                  Up interface & addr

F Lo2 10.1.1.2/24                         Lo1 10.1.1.1/24
```

The following is sample output from the **show arm ipv4 conflicts** command with the **unnumbered** keyword:

```
RP/0/RP0/CPU0:router# show arm ipv4 conflicts unnumbered

Forced down interface          Up interface                  VRF
tu2->tu1                       tu1->Lo1
```

This table describes the significant fields shown in the display.

Table 50: show arm conflicts Command Field Descriptions

Field	Description
Forced down	Legend defining a symbol that may appear in the output for this command.
Down interface & addr	Forced down interface name, type, and address.
Up interface & addr	List of interfaces that are up.
Forced down interface	Unnumbered interfaces that are in conflict and forced down.
Up interface	Unnumbered interfaces that are in conflict and are up.

show arm registrations producers

To display producer registration information for the Address Repository Manager (ARM), use the **show arm registrations producers** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} **registrations producers**

Syntax Description

ipv4	Displays IPv4 producer registration information.
ipv6	Displays IPv6 producer registration information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show arm registrations producers** command to display information on producers of IP ARM registrations. Registration information is displayed with the ID.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm ipv4 registrations producers** command:

```
Routers# show arm ipv4 registrations producers

Id    Node            Producer Id   IPC Version Connected?
0     0/0/0           ipv4_io       1.1         Y
4     0/1/0           ipv4_io       1.1         Y
3     0/2/0           ipv4_io       1.1         Y
2     0/4/0           ipv4_io       1.1         Y
1     0/6/0           ipv4_io       1.1         Y
```

This table describes the significant fields shown in the display.

Table 51: show arm registrations producers Command Field Descriptions

Field	Description
Id	An identifier used by the IP Address ARM (IP ARM) to keep track of the producer of the IP address.
Node	The physical node (RP/LC CPU) where the producer is running.
Producer Id	The string used by the producer when registering with IP ARM.

Field	Description
IPC Version	Version of the apis used by the producer to communicate with IP ARM.
Connected?	Status of whether the producer is connected or not.

show arm database

To display IPv4 or IPv6 address information stored in the Address Repository Manager (ARM) database, use the **show arm database** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} [**vrf** *{vrf-name}*] **database** [**interface** *type interface-path-id* | **network** *prefix/ length*]

Syntax Description

ipv4	Displays IPv4 address information.
ipv6	Displays IPv6 address information.
vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
interface	(Optional) Displays the IPv4 or IPv6 address configured on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
network	(Optional) Displays addresses that match a prefix.
prefix / length	(Optional) Network prefix and mask. A slash (/) must precede the specified mask. The range is from 0 to 128.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show arm database** command should be used to display information in the IP ARM database. Database information is displayed with the IPv4 or IPv6 address, interface type and name, and producer information.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm database** command:

```
RP/0/RP0/CPU0:router# show arm
ipv4 database interface loopback database
Fri Jul 25 10:54:52.304 PST DST

P = Primary, S = Secondary address
|U = Unnumbered
|| Address            Interface                      Producer

VRF: default
P  172.29.52.75/24    MgmtEth0/RP0/CPU0/0            ipv4_ma 0/RP0/CPU0           100
P  10.2.2.2/32        Loopback0                      ipv4_ma 0/RP1/CPU0
P  10.12.24.2/24      Bundle-POS24                   ipv4_ma 0/RP1/CPU0
P  10.12.28.2/24      Bundle-Ether28                 ipv4_ma 0/RP1/CPU0
P  10.12.29.2/24      Bundle-Ether28.1               ipv4_ma 0/RP1/CPU0
P  10.12.30.2/24      Bundle-Ether28.2               ipv4_ma 0/RP1/CPU0
P  10.12.31.2/24      Bundle-Ether28.3               ipv4_ma 0/RP1/CPU0
P  10
.1
.1
.s
/24   Loopback1ipv4_io 0/0/0P  10.1
.1
.1
/24 Loopback1  ipv4_io 0/0/0

| Address             Interface  Producer
P  10.12.16.2/24      GigabitEthernet0/1/5/0         ipv4_ma 0/1/CPU0           1001
P  10.23.4.2/24       GigabitEthernet0/1/5/1         ipv4_ma 0/1/CPU0           1002
P  10.27.4.2/24       GigabitEthernet0/1/5/2         ipv4_ma 0/1/CPU0
P  10.12.8.2/24       POS0/1/0/1                     ipv4_ma 0/1/CPU0
P  10.112.4.2/24      POS0/1/0/2                     ipv4_ma 0/1/CPU0
P  10.112.8.2/24      POS0/1/0/3                     ipv4_ma 0/1/CPU0
P  10.12.32.2/24      POS0/1/4/2                     ipv4_ma 0/1/CPU0
P  10.12.32.2/24      POS0/1/4/3                     ipv4_ma 0/1/CPU0
P  172.29.52.28/24    MgmtEth0/4/CPU1/0              ipv4_ma 0/4/CPU1
P  172.29.52.27/24    MgmtEth0/4/CPU0/0              ipv4_ma 0/4/CPU0
P  10.12.20.2/24      GigabitEthernet0/6/5/1         ipv4_ma 0/6/CPU0
P  10.4
.1
.4
/24 gigabitethernet 10/0 ipv4_io 1 10
S 10.4.2.4/24         gigabitethernet 10/0  ipv4_io 1 10
S 10.4.3.4/24         gigabitethernet 10/1  ipv4_io 1 10

P = Primary, S = Secondary address

|U = Unnumbered

|| Address            Interface                      Producer
VRF: default
P  10.12.12.2/24      POS0/6/0/1                     ipv4_ma 0/6/CPU0
P  10.23.8.2/24       POS0/6/4/4                     ipv4_ma 0/6/CPU0
P  10.12.4.2/24       POS0/6/4/5                     ipv4_ma 0/6/CPU0
P  10.24.4.2/24       POS0/6/4/6                     ipv4_ma 0/6/CPU0
P  12
.25.12
.10/16 MgmtEth0/RSP0/CPU0/0  ipv4_ma 0/RSP0/CPU0
```

This table describes the significant fields shown in the display.

Table 52: show arm database Command Field Descriptions

Field	Description
Primary	Primary IP address.
Secondary	Secondary IP address.
Unnumbered Address	Interface is unnumbered and the address displayed is that of the referenced interface.
Interface	Interface that has this IP address.
Producer	Process that provides the IP address to the ARM.

show arm router-ids

To display the router identification information with virtual routing and forwarding table information for the Address Repository Manager (ARM), use the **show arm router-ids** command in XR EXEC mode.

show arm [**ipv4**] **router-ids**

Syntax Description

ipv4	(Optional) Displays IPv4 router information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show arm router-ids** command with the **ipv4** keyword to display the selected router ID information for the router.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm router-ids** command:

```
RP/0/RP0/CPU0:router# show arm router-ids

Router-ID          Interface

10.10.10.10        Loopback0
```

This table describes the significant fields shown in the display.

Table 53: show arm router-ids Command Field Descriptions

Field	Description
Router-ID	Router identification.
Interface	Interface identification.

show arm summary

To display summary information for the IP Address Repository Manager (ARM), use the **show arm summary** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} **summary**

Syntax Description

ipv4	Displays IPv4 summary information.
ipv6	Displays IPv6 summary information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show arm summary** command to display a summary of the number of producers, address conflicts, and unnumbered interface conflicts in the router.

Task ID

Task ID	Operations
network	read

Examples

The following is sample output from the **show arm summary** command:

```
Router# show arm ipv4 summary

IPv4 Producers                          :          1
IPv4 address conflicts                  :          0
IPv4 unnumbered interface conflicts     :          0
IPv4 VRF known                          :          0
IPv4 DB Master version                  : 0x00000000
```

This table describes the significant fields shown in the display.

Table 54: show arm summary Command Field Descriptions

Field	Description
IPv4 Producers	Number of IPv4 producers on the router.
IPv4 address conflicts	Number of IPv4 address conflicts on the router.
IPv4 unnumbered interface conflicts	Number of IPv4 conflicts on unnumbered interfaces.

Field	Description
IPv4 DB Master version	IPv4 DB Master version

show arm vrf-summary

To display a summary of VPN routing and forwarding (VRF) instance information identified by the Address Repository Manager (ARM), use the **show arm vrf-summary** command in XR EXEC mode.

show arm {**ipv4** | **ipv6**} **vrf-summary**

Syntax Description

ipv4	Displays IPv4 address information.
ipv6	Displays IPv6 address information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show arm vrf-summary** command to display information about an IPv4 VPN routing and forwarding instance.

Task ID

Task ID	Operations
network	read

Examples

The following example is output from the **show arm vrf-summary** command:

```
RP/0/RP0/CPU0:router# show arm vrf-summary

VRF IDs:        VRF-Names:
0x60000000      default
0x60000001      vrf1
0x60000002      vrf2
```

This table describes the significant fields shown in the display.

Table 55: show arm vrf-summary Command Field Descriptions

Field	Description
VRF IDs	VPN routing and forwarding (VRF) identification (vrfid) number.
VRF-Names	Name given to the VRF.

show clns statistics

To display Connectionless Network Service (CLNS) protocol statistics, use the **show clns statistics** command in XR EXEC mode.

show clns statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use this command to display CLNS statistics.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show clns statistics** command:

```
RP/0/RP0/CPU0:router# show clns statistics

CLNS Statistics:
Last counter clear:                    2868 seconds ago
Total number of packets sent:          0
Total number of packets received:      0
Send packets dropped, buffer overflow: 0
Send packets dropped, out of memory:   0
Send packets dropped, other:           0
Receive socket max queue size:         0
Class    Overflow/Max   Rate Limit/Max
IIH             0/0              0/0
LSP             0/0              0/0
SNP             0/0              0/0
OTHER           0/0              0/0
Total          0                0
```

This table describes the significant fields shown in the display.

Table 56: show clns traffic Command Field Descriptions

Field	Description
Class	Indicates the packet type. Packets types are as follows: • IIH—Intermediate System-to-Intermediate-System hello packets • lsp—Link state packets • snp—Sequence number packets • other
Overflow/Max	Indicates the number of packet drops due to the socket queue being overflown. The count displays in an *x/y* format where *x* indicates the total number of packet drops and *y* indicates the maximum number of drops in a row.
Rate Limit/Max	Indicates the number of packet drops due to rate limitation. The count displays in an *x/y* format where *x* indicates the total number of packet drops and *y* indicates the maximum number of drops in a row.

show hw-module local-station-mac

To display status of local station MAC address in the router, use the **show hw-module local-station-mac** command in XR EXEC mode.

show hw-module local-station-mac

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

Use the **show hw-module local-station-mac** command to display status of the local station MAC address in the router..

Task ID

Task ID	Operations
network	read

Examples

The following example is output from the **show hw-module local-station-mac** command:

```
Router# show hw-module local-station-mac
--------------------------------------------------------------
Knob                          Status         Applied   Action
--------------------------------------------------------------
Local-Station-MAC             Configured     Yes       None
```

show ipv4 interface

To display the usability status of interfaces configured for IPv4, use the **show ipv4 interface** command in the XR EXEC mode.

show **ipv4** [**vrf** *vrf-name*] **interface** [*type* *interface-path-id* | **brief** | **summary**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays the primary IPv4 addresses configured on the router's interfaces and their protocol and line states.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

If VRF is not specified, the software displays the default VRF.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show ipv4 interface** command provides output similar to the **show ipv6 interface** command, except that it is IPv4-specific.

The interface name will be displayed only if the name belongs to the VRF instance. If the *vrf-name* is not specified then the interface instance will be displayed only if the interface belongs to the default VRF.

Task ID

Task ID	Operations
ipv4	read
network	read

Examples

This is the sample output of the **show ipv4 interface** command:

```
RP/0/RP0/CPU0:router# show ipv4 interface

Bundle-Ether1 is Down, ipv4 protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet address is 40.30.1.2/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
Bundle-Ether2 is Down, ipv4 protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet address is 40.30.2.2/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
Bundle-Ether10 is Shutdown, ipv4 protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet protocol processing disabled
Bundle-Ether54 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.0.9.0/31
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1 224.0.0.2
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
Bundle-Ether1900 is Down, ipv4 protocol is Down
```

```
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.0.54.1/30
  MTU is 9000 (8986 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
Bundle-Ether1901 is Down, ipv4 protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.0.55.1/30
  MTU is 9000 (8986 is available to IP)
```

This table describes the significant fields shown in the display.

Table 57: show ipv4 interface Command Field Descriptions

Field	Description
Loopback0 is Up	If the interface hardware is usable, the interface is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is Up	If the interface can provide two-way communication, the line protocol is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address	IPv4 Internet address and subnet mask of the interface.
Secondary address	Displays a secondary address, if one has been set.
MTU	Displays the IPv4 MTU[8] value set on the interface.
Multicast reserved groups joined	Indicates the multicast groups this interface belongs to.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled or disabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether proxy ARP[9] is enabled or disabled on an interface.
ICMP redirects	Specifies whether ICMPv4[10] redirects are sent on this interface.
ICMP unreachables	Specifies whether unreachable messages are sent on this interface.
Internet protocol processing disabled	Indicates an IPv4 address has not been configured on the interface.

[8] MTU = maximum transmission unit

[9] ARP = Address Resolution Protocoladdress resolution protocol

[10] ICMPv4 = Internet Control Message Protocol internet control message protocol version 4

show ipv4 traffic

To display the IPv4 traffic statistics, use the **show ipv4 traffic** command in the XR EXEC mode.

show ipv4 traffic [**brief**]

Syntax Description

brief	(Optional) Displays only IPv4 and Internet Control Message Protocol version 4 (ICMPv4) traffic.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show ipv4 traffic** command provides output similar to the **show ipv6 traffic** command, except that it is IPv4-specific.

Task ID

Task ID	Operations
ipv4	read
network	read

Examples

This is the sample output of the **show ipv4 traffic** command:

```
RP/0/RP0/CPU0:router# show ipv4 traffic

IP statistics:
  Rcvd:  486522 total, 55292 local destination
         0 format errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad source, 0 bad header
         842 with options, 0 bad, 0 unknown
  Opts:  0 end, 0 nop, 0 basic security, 0 extended security
         0 strict source rt, 0 loose source rt, 0 record rt
         0 stream ID, 0 timestamp, 842 alert, 0 cipso
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble, 0 fragments received
         0 fragmented, 0 fragment count, 0 fragment max drop
  Bcast: 0 sent, 0 received
  Mcast: 13042 sent, 417434 received
   Lisp: 0 encapped in v4, 0 decapped from v4
         0 encapped in v6, 0 decapped from v6
         0 encap errors, 0 decap errors
   Drop: 0 encapsulation failed, 19 no route, 0 too big
   Sent: 446780 total

ICMP statistics:
  Sent: 0 admin unreachable, 190147 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        190147 total
  Rcvd: 0 admin unreachable, 11 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 redirect, 0 parameter error
        0 source quench, 0 timestamp, 0 timestamp reply
        0 router advertisement, 0 router solicitation
        11 total, 0 checksum errors, 0 unknown

UDP statistics:
        424354 packets input, 10881 packets output
        0 checksum errors, 13236 no port
        0 forwarded broadcasts

TCP statistics:
        53775 packets input, 56104 packets output
        0 checksum errors, 0 no port
```

This table describes the significant fields shown in the display.

Table 58: show ipv4 traffic Command Field Descriptions

Field	Description
bad hop count	Occurs when a packet is discarded because its TTL[11] field was decremented to zero.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
IP statistics Rcvd total	Indicates the total number of local destination and other packets received in the software plane. It does not account for the IP packets forwarded or discarded in hardware.
no route	Counted when the Cisco IOS XR software discards a datagram it did not know how to route.

[11] TTL = time-to-live

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in the XR EXEC mode.

show **ipv6** [**vrf** *vrf-name*] **interface** [**summary** | [*type* *interface-path-id*][**brief** [**link-local** | **global**]]]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
link-local	(Optional) Displays the link local IPv6 address.
global	(Optional) Displays the global IPv6 address.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show ipv4 interface** command, except that it is IPv6-specific.

Use the **link-local** or **global** keywords along with the **brief** keyword to view the link local or global IPv6 addresses.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 interface** command:

```
RP/0/RP0/CPU0:router# show ipv6 interface
  Bundle-Ether1 is Down, ipv6 protocol is Down, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::e448:5cff:fe10:b484 [TENTATIVE]
  Global unicast address(es):
    40:30:1:1::2, subnet is 40:30:1:1::/64 [TENTATIVE]
  Joined group address(es): ff02::2 ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 160 to 240 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  common access list is not set, access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

This table describes the significant fields shown in the display.

Table 59: show ipv6 interface Command Field Descriptions

Field	Description
Bundle-Ether1 is Down	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.

Field	Description
line protocol is Up (or down)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful). If the interface can provide two-way communication, the line protocol is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.
TENTATIVE	The state of the address in relation to duplicate address detection. States can be any of the following: • duplicate—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface. • tentative—Duplicate address detection is either pending or under way on this interface. **Note** If an address does not have one of these states (the state for the address is blank), the address is unique and is being used.
Global unicast addresses	Displays the global unicast addresses assigned to the interface.
ICMP redirects	State of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	State of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

This is the sample output of the **show ipv6 interface brief link-local** command:

```
RP/0/RP0/CPU0:router#show ipv6 interface brief link-local

Interface                IPv6-Address                 Status     Protocol
Bundle-Ether1            fe80::e448:5cff:fe10:b484    Down       Down
Bundle-Ether2            fe80::e448:5cff:fe10:b483    Down       Down
Bundle-Ether10           unassigned                   Shutdown   Down
Bundle-Ether54           fe80::e448:5cff:fe10:b481    Up         Up
Bundle-Ether1900         fe80::e448:5cff:fe10:b48a    Down       Down
Bundle-Ether1901         fe80::e448:5cff:fe10:b489    Down       Down
Bundle-Ether1902         fe80::e448:5cff:fe10:b488    Down       Down
```

```
Bundle-Ether1903          fe80::e448:5cff:fe10:b487     Down       Down
Bundle-Ether1904          fe80::e448:5cff:fe10:b486     Down       Down
Bundle-Ether1905          unassigned                    Shutdown   Down
Bundle-Ether1906          fe80::e448:5cff:fe10:b48e     Down       Down
Loopback0                 fe80::9d4c:a5ff:fe2f:2615     Up         Up
Loopback1                 fe80::9d4c:a5ff:fe2f:2615     Up         Up
tunnel-te54               unassigned                    Down       Down
tunnel-te718              unassigned                    Up         Up
tunnel-te720              unassigned                    Up         Up
tunnel-te5454             unassigned                    Up         Up
MgmtEth0/RP0/CPU0/0       unassigned                    Up         Up
HundredGigE0/2/0/0        unassigned                    Shutdown   Down
HundredGigE0/2/0/1        unassigned                    Shutdown   Down
HundredGigE0/2/0/2        unassigned                    Shutdown   Down
HundredGigE0/2/0/3        unassigned                    Shutdown   Down
HundredGigE0/2/0/4        fe80::e448:5cff:fe10:b130     Shutdown   Down
HundredGigE0/2/0/5        unassigned                    Shutdown   Down
HundredGigE0/2/0/6        unassigned                    Shutdown   Down
HundredGigE0/2/0/7        unassigned                    Shutdown   Down
HundredGigE0/2/0/8        unassigned                    Down       Down
HundredGigE0/2/0/9        unassigned                    Shutdown   Down
HundredGigE0/2/0/10       unassigned                    Shutdown   Down
HundredGigE0/2/0/11       unassigned                    Shutdown   Down
HundredGigE0/2/0/12       unassigned                    Shutdown   Down
HundredGigE0/2/0/13       unassigned                    Shutdown   Down
HundredGigE0/2/0/15       unassigned                    Shutdown   Down
HundredGigE0/2/0/16       unassigned                    Shutdown   Down
HundredGigE0/2/0/17       unassigned                    Shutdown   Down
HundredGigE0/2/0/18       unassigned                    Shutdown   Down
HundredGigE0/2/0/19       unassigned                    Shutdown   Down
HundredGigE0/2/0/20       unassigned                    Shutdown   Down
HundredGigE0/2/0/21       unassigned                    Shutdown   Down
HundredGigE0/2/0/22       unassigned                    Shutdown   Down
HundredGigE0/2/0/23       unassigned                    Shutdown   Down
HundredGigE0/2/0/25       fe80::e448:5cff:fe10:b184     Shutdown   Down
HundredGigE0/2/0/26       unassigned                    Shutdown   Down
HundredGigE0/2/0/27       unassigned                    Shutdown   Down
HundredGigE0/2/0/28       unassigned                    Shutdown   Down
HundredGigE0/2/0/29       unassigned                    Shutdown   Down
HundredGigE0/2/0/31       unassigned                    Shutdown   Down
HundredGigE0/2/0/32       unassigned                    Shutdown   Down
HundredGigE0/2/0/33       unassigned                    Shutdown   Down
HundredGigE0/2/0/34       unassigned                    Shutdown   Down
HundredGigE0/2/0/35       unassigned                    Shutdown   Down
TenGigE0/2/0/14/0         unassigned                    Up         Up
TenGigE0/2/0/14/1         unassigned                    Up         Up
TenGigE0/2/0/14/2         unassigned                    Up         Up
TenGigE0/2/0/14/3         unassigned                    Up         Up
TenGigE0/2/0/24/0         fe80::e448:5cff:fe10:b180     Up         Up
```

This is the sample output of the **show ipv6 interface brief global** command:

```
RP/0/#show ipv6 interface brief global

Interface           IPv6-Address                  Status     Protocol
Bundle-Ether54            10:0:9::2                     Up         Up
Bundle-Ether1900          10:0:54::2                    Up         Up
Bundle-Ether1901          10:0:55::2                    Up         Up
Bundle-Ether1902          10:0:56::2                    Up         Up
Bundle-Ether1903          10:0:84::2                    Up         Up
Bundle-Ether1904          10:0:85::2                    Up         Up
Bundle-Ether1906          10:0:86::2                    Up         Up
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief link-local** command:

```
RP/0/RP0/CPU0:router#show ipv6 interface tenGigE 0/0/0/0 brief link-local

Interface                 IPv6-Address                  Status     Protocol
HundredGigE0/0/0/0    fe80::fe:8ff:fecb:26c5        Up         Up
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief global** command:

```
RP/0/RP0/CPU0:router#show ipv6 interface tenGigE 0/0/0/0 brief global

Interface                 IPv6-Address                  Status     Protocol
HundredGigE0/0/0/0    2001:db8::1                   Up         Up
```

show ipv6 neighbors

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in the XR EXEC mode.

show ipv6 neighbors [*type interface-path-id* | **location** *node-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface instance or a virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Designates a node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

All IPv6 neighbor discovery cache information is displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 neighbors** command when entered with an interface type and number:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors HundredGigE0/0/0/2

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH tenGigE
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH tenGigE
3001:1::45a                                 - 0002.7d1a.9472  REACH tenGigE
```

This is the sample output of the **show ipv6 neighbors** command:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors

IPv6 Address                             Age Link-layer Addr State Interface
Location
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/2/0/25
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/2/0/4
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Te0/2/0/30/3
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/2/0/30/2
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/2/0/30/1
0/2/CPU0
fe80::d66d:50ff:fe38:9544                97   d46d.5038.9544 REACH Te0/2/0/30/0
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/2/0/30/0
0/2/CPU0
10:0:8::2                                89   10f3.114c.719c REACH Te0/2/0/24/0
0/2/CPU0
fe80::12f3:11ff:fe4c:719c                135  10f3.114c.719c REACH Te0/2/0/24/0
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/2/0/24/0
0/2/CPU0
10:0:9::2                                150  e607.2b8d.3484 REACH BE54
0/2/CPU0
fe80::e407:2bff:fe8d:3484                149  e607.2b8d.3484 REACH BE54
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH BE54
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1900
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1901
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1903
0/2/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1904
0/2/CPU0
1000::2                                  50   0010.9400.000d REACH Hu0/4/0/0
0/4/CPU0
fe80::1                                  153  0010.9400.000d REACH Hu0/4/0/0
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Hu0/4/0/0
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/4/0/6
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/4/0/18
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/4/0/25
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/4/0/30/0
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Te0/4/0/30/1
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1901
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1902
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1903
0/4/CPU0
```

```
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1906
0/4/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/6/0/35
0/6/CPU0
200:1::2                                 157  0010.9400.0013 REACH Hu0/6/0/34
0/6/CPU0
fe80::1                                  130  0010.9400.0013 REACH Hu0/6/0/34
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 REACH Hu0/6/0/34
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/6/0/16
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/6/0/18
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/6/0/19
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/6/0/20
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Hu0/6/0/21
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Te0/6/0/2/2
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE Te0/6/0/2/1
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE2
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1900
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1902
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1904
0/6/CPU0
[Mcast adjacency]                           - 0000.0000.0000 DELETE BE1906
0/6/CPU0
```

This is the sample output of the **show ipv6 neighbors** command when entered with a location:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors location 0/2/CPU0

IPv6 Address    Age Link-layer Addr State Interface     Location
2001:3::2       119  0013.9400.0002 REACH BE3           0/2/CPU0
2001:3::3       179  0013.9400.0003 DELAY BE3           0/2/CPU0
2001:3::4       166  0013.9400.0004 REACH BE3           0/2/CPU0
2001:3::5       78   0013.9400.0005 REACH BE3           0/2/CPU0
2001:3::6       19   0013.9400.0006 REACH BE3           0/2/CPU0
2001:3::7       173  0013.9400.0007 REACH BE3           0/2/CPU0
2001:3::8       140  0013.9400.0008 REACH BE3           0/2/CPU0
2001:3::9       163  0013.9400.0009 REACH BE3           0/2/CPU0
2001:3::a       40   0013.9400.000a REACH BE3           0/2/CPU0
2001:3::b       90   0013.9400.000b REACH BE3           0/2/CPU0
2001:3::c       35   0013.9400.000c REACH BE3           0/2/CPU0
2001:3::d       114  0013.9400.000d REACH BE3           0/2/CPU0
2001:3::e       117  0013.9400.000e REACH BE3           0/2/CPU0
2001:3::f       157  0013.9400.000f REACH BE3           0/2/CPU0
2001:3::10      9    0013.9400.0010 REACH BE3           0/2/CPU0
2001:3::11      120  0013.9400.0011 REACH BE3           0/2/CPU0
2001:3::12      87   0013.9400.0012 REACH BE3           0/2/CPU0
2001:3::13      180  0013.9400.0013 DELAY BE3           0/2/CPU0
2001:3::14      103  0013.9400.0014 REACH BE3           0/2/CPU0
2001:3::15      132  0013.9400.0015 REACH BE3           0/2/CPU0
2001:3::16      33   0013.9400.0016 REACH BE3           0/2/CPU0
2001:3::17      150  0013.9400.0017 REACH BE3           0/2/CPU0
2001:3::18      117  0013.9400.0018 REACH BE3           0/2/CPU0
```

```
2001:3::19      48   0013.9400.0019 REACH BE3          0/2/CPU0
2001:3::1a      67   0013.9400.001a REACH BE3          0/2/CPU0
2001:3::1b      91   0013.9400.001b REACH BE3          0/2/CPU0
2001:3::1c      33   0013.9400.001c REACH BE3          0/2/CPU0
2001:3::1d      174  0013.9400.001d DELAY BE3          0/2/CPU0
2001:3::1e      144  0013.9400.001e REACH BE3          0/2/CPU0
2001:3::1f      121  0013.9400.001f REACH BE3          0/2/CPU0
2001:3::20      53   0013.9400.0020 REACH BE3          0/2/CPU0
```

This table describes significant fields shown in the display.

Table 60: show ipv6 neighbors Command Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.
State	The state of the neighbor cache entry. These are the states for dynamic entries in the IPv6 neighbor discovery cache: • INCMP (incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • reach (reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in reach state, the device takes no special action as packets are sent. • stale—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in stale state, the device takes no action until a packet is sent. • delay—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the delay state, send a neighbor solicitation message and change the state to probe. • probe—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. These are the possible states for static entries in the IPv6 neighbor discovery cache: • reach (reachable)—The interface for this entry is up. • INCMP (incomplete)—The interface for this entry is down. **Note** Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (incomplete) and reach (reachable) states are different for dynamic and static cache entries.
Interface	Interface from which the address is reachable.

show ipv6 neighbors summary

To display summary information for the neighbor entries, use the **show ipv6 neighbors summary** command in the XR EXEC mode.

show ipv6 neighbors summary

Syntax Description

This command has no keywords or arguments.

Command Default

The default value is disabled.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
ipv6	read

Examples

This is the sample output of the **show ipv6 neighbors summary** command that shows the summary information for the neighbor entries:

```
XR EXEC mode# show ipv6 neighbors summary

Mcast nbr entries:
    Subtotal: 0
Static nbr entries:
    Subtotal: 0
Dynamic nbr entries:
    Subtotal: 0

Total nbr entries: 0
```

show ipv6 path-mtu

To display path maximum transmission unit (MTU) details of IPv6 packets, use the **show ipv6 path-mtu** command in the XR Config mode.

show ipv6 path-mtu [**vrf** { *vrf-name* | **all**} [**location** *node-id*]] [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) The designated node. The node-id argument is entered in the *rack/slot/module* notation.

Command Default

None.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If the location option is specified, only the details of the node specified in the **location** *node-id* keyword and argument are displayed. Path MTU discovery for IPv6 packets is supported only for applications using TCP and Ping protocol.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

Examples

This example shows how to display path MTU details of IPv6 packets:

```
RP/0/RP0/CPU0:router(config)#  show ipv6 pmtu

Destination         Ifhandle        Vrfid               Path Mtu       Time Left
bb::1               0x300           0x60000000          1300           00:01:27
cd::1               0x300           0x60000000          1300           00:01:42
```

show ipv6 traffic

To display the IPv6 traffic statistics, use the **show traffic** command in the XR EXEC mode.

show ipv6 traffic [**brief**]

Syntax Description

brief	(Optional) Displays only IPv6 and Internet Control Message Protocol version 6 (ICMPv6) traffic statistics.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show ipv6 traffic** command provides output similar to the **show ipv4 traffic** command, except that it is IPv6-specific.

Task ID

Task ID	Operations
ipv6	read
network	read

Examples

This is the sample output of the **show ipv6 traffic** command:

```
RP/0/RP0/CPU0:router# show ipv6 traffic

 IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 reassembly max drop
         0  sanity address check drops
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor,
                 0 address, 0 port, 0 unknown
        parameter: 0 error, 0 header, 0 option,
                   0 unknown
        0 hopcount expired, 0 reassembly timeout,
        0 unknown timeout, 0 too big,
        0 echo request, 0 echo reply
  Sent: 0 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor,
                 0 address, 0 port, 0 unknown
        parameter: 0 error, 0 header, 0 option
                 0 unknown
        0 hopcount expired, 0 reassembly timeout,
        0 unknown timeout, 0 too big,
        0 echo request, 0 echo reply

Neighbor Discovery ICMP statistics:
  Rcvd: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert
  Sent: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert

UDP statistics:
        0 packets input, 0 checksum errors
        0 length errors, 0 no port, 0 dropped
        0 packets output

TCP statistics:s
        0 packets input, 0 checksum errors, 0 dropped
        0 packets output, 0 retransmitted
```

This table describes the significant fields shown in the display.

Table 61: show ipv6 traffic Command Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
total	Total number of packets received by the software.
local destination	Locally destined packets received by the software.
source-routed	Packets seen by the software with RH.
truncated	Truncated packets seen by the software.
bad header	An error was found in generic HBH, RH, DH, or HA. Software only.
unknown option	Unknown option type in IPv6 header.
unknown protocol	Protocol specified in the IP header of the received packet is unreachable.
Sent:	Statistics in this section refer to packets sent by the router.
forwarded	Packets forwarded by the software. If the packet cannot be forwarded in the first lookup (for example, the packet needs option processing), then the packet is not included in this count, even if it ends up being forwarded by the software.
Mcast:	Multicast packets.

Field	Description
ICMP statistics:	Internet Control Message Protocol statistics.

show linux networking interfaces address-only

To display virtual IP addresses and IP addresses for address-only interfaces, use the **show linux networking interfaces address-only** command in the XR EXEC mode. Address-only interfaces are those interfaces whose addresses are copied to the Linux loopback device by XLNC (XR Linux networking coordinator).

show linux networking interfaces address-only

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.2	The virtual IP addresses are displayed in the output of the command.
Release 7.3.2	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operations
system	read

Example

This is the sample output of the **show linux networking interfaces address-only** command:

```
Router# show linux networking interfaces address-only
The following interface addresses have been added to the Linux loopback device for L3
reachability.

VRF default
----------------------------------------------
MgmtEth0/RP0/CPU0/0
    IPv4: 10.0.0.3 (virtual address)
    IPv6: 10::3 (virtual address)
```

show local pool

To display IPv4 local pool details, use the **show local pool** command in XR EXEC mode.

show {**local***other_pool_types*} **pool** [**vrf** *vrf_name*] {**ipv4** | **ipv6**} {**default***poolname*}

Syntax Description

local	Specifies that the address pool is local.
vrf	Specifies that a VRF name will be given. If is parameter is missing, the default VRF is assumed.
vrf_name	Specifies the name of the VRF to which the addresses of the pool belongs. If no name is given, the default VRF is assumed.
default	Creates a default local IPv4 address pool that is used if no other pool is named.
poolname	Specifies the name of the local IPv4 address pool.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Syntax Description

This command has no keywords or arguments.

Task ID

Task ID	Operations
ipv4	read
network	read

Examples

The following is sample output from the **show ipv4 local pool** with a poolname of P1:

```
RP/0/RP0/CPU0:router# show ipv4 local pool P1

Pool Begin End FreeInUse
P1 172.30.228.11172.30.228.1660
Available addresses:
172.30.228.11
172.30.228.12
172.30.228.13
172.30.228.14
172.30.228.15
172.30.228.16
Inuse addresses:
None
```

This table describes the significant fields shown in the display.

Table 62: show ipv4 local pool Command Descriptions

Field	Description
Pool	Name of the pool.
Begin	First IP address in the defined range of addresses in this pool.
End	Last IP address in the defined range of addresses in this pool.
Free	Number of addresses available.
InUse	Number of addresses in use.

show mpa client

To display information about the Multicast Port Arbitrator (MPA) clients, use the **show mpa client** command in XR EXEC mode.

show mpa client {**consumers** | **producers**}

Syntax Description

consumers	Displays the clients for the consumers.
producers	Displays the clients for the producers.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
network	read

Examples

The following sample output is from the **show mpa client** command:

```
RP/0/RP0/CPU0:router# show mpa client consumers

List of producer clients for ipv4 MPA

Location      Protocol      Process
0/1/CPU0      255           raw
0/1/CPU0      17            udp
0/4/CPU0      17            udp
0/4/CPU0      255           raw
0/4/CPU1      17            udp
0/4/CPU1      255           raw
0/6/CPU0      17            udp
0/6/CPU0      255           raw
0/RP1/CPU0    17            udp
0/RP1/CPU0    255           raw
```

show mpa groups

To display Multicast Port Arbitrator (MPA) multicast group information, use the **show mpa groups** command in XR EXEC mode .

show **mpa** **groups** *type* *interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0 /CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
network	read

Examples

The following sample output is from the **show mpa groups** command:

```
RP/0/RP0/CPU0:router# show mpa groupsHundredGigE0/0/0/2
Mon Jul 27 04:07:19.802 DST
HundredGigE0/0/0/2 :-
```

```
224.0.0.1 : includes 0, excludes 1, mode EXCLUDE
  <no source filter>
224.0.0.2 : includes 0, excludes 1, mode EXCLUDE
  <no source filter>
224.0.0.5 : includes 0, excludes 1, mode EXCLUDE
  <no source filter>
224.0.0.6 : includes 0, excludes 1, mode EXCLUDE
  <no source filter>
224.0.0.13 : includes 0, excludes 1, mode EXCLUDE
  <no source filter>
224.0.0.22 : includes 0, excludes 1, mode EXCLUDE
  <no source filter>
```

show mpa ipv4

To display information for Multicast Port Arbitrator (MPA) for IPv4, use the **show mpa ipv4** command in XR EXEC mode.

show mpa ipv4 {**client** {**consumers** | **producers**} | **groups** *type interface-path-id* | **trace**}

Syntax Description

client	Displays information about the MPA clients.
consumers	Displays the clients for the consumers.
producers	Displays the clients for the producers.
groups	Displays information about the MPA multicast group.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RSP0) and the module is CPU0. Example: interface MgmtEth0/RSP0/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
trace	Displays MPA trace information

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
network	read

Examples

The following sample output is from the **show mpa ipv4** command:

```
RP/0/RP0/CPU0:router# show mpa ipv4 client producers

List of producer clients for ipv4 MPA

 Location     Protocol     Process
 0/1/CPU0     17           udp
 0/1/CPU0     255          raw
 0/4/CPU0     17           udp
 0/4/CPU0     255          raw
 0/4/CPU1     17           udp
 0/4/CPU1     255          raw
 0/6/CPU0     17           udp
 0/6/CPU0     255          raw
 0/RP0/CPU0   17           udp
 0/RP0/CPU0   255          raw
 0/RP1/CPU0   255          raw
 0/RP1/CPU0   17           udp
```

show mpa ipv6

To display information for Multicast Port Arbitrator (MPA) for IPv6, use the **show mpa ipv6** command in XR EXEC mode.

show mpa ipv6 {**client** {**consumers** | **producers**} | **groups** *type interface-path-id*}

Syntax Description

client	Displays information about the MPA clients.
consumers	Displays the clients for the consumers.
producers	Displays the clients for the producers.
groups	Displays information about the MPA multicast group.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. • *rack*: Chassis number of the rack. • *slot*: Physical slot number of the modular services card or line card. • *module*: Module number. A physical layer interface module (PLIM) is always 0. • *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
network	read

Examples

The following sample output is from the **show mpa ipv6** command:

```
RP/0/RP0/CPU0:router# show mpa ipv6 client producers

List of producer clients for ipv6 MPA

 Location      Protocol      Process

 0/RP1/CPU0    17            udp
 0/RP1/CPU0    255           raw
```

show hw-module profile route-scale

To display the status of the configured IPv6 prefix scale expansion feature, run the **show hw-module profile route-scale** command in XR EXEC mode.

show hw-module profile route-scale

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

The chassis must be reloaded for the **hw-module** command to be functional.

Task ID

Task ID	Operations
ipv6	read, write

After the configuration of the hw-module profile route scale ipv6-unicast connected-prefix high command is complete, reload the router for the feature to take effect. The `Applied` column in the **show hw-module profile route-scale** command displays *No* if the line card is not reloaded.

```
Router# show hw-module profile route-scale
Tue Aug 23 18:27:03.551 UTC
--------------------------------------------------------------
Knob                          Status          Applied   Action
--------------------------------------------------------------
Route-Scale                   Configured      No        Reload
```

After you reload the router for the feature to take effect, the `Applied` column displays *Yes*.

```
Router# reload location all
Tue Aug 23 18:27:56.482 UTC
Proceed with reload? [confirm] y
```

```
Router# show hw-module profile route-scale
Tue Aug 23 18:33:47.768 UTC
--------------------------------------------------------------
Knob                          Status          Applied   Action
--------------------------------------------------------------
Route-Scale                   Configured      Yes       None
```

Transport Stack Commands

This chapter describes the Cisco IOS XR software commands used to configure and monitor features related to the transport stack (Nonstop Routing, Stream Control Transmission Protocol (SCTP), NSR, TCP, User Datagram Protocol (UDP), and RAW. Any IP protocol other than TCP or UDP is known as a *RAW* protocol.

For detailed information about transport stack concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Command Reference for Cisco 8000 Series Routers*

clear nsr ncd client

To clear the counters of a specified client or all the clients of nonstop routing (NSR) Consumer Demuxer (NCD), use the **clear nsr ncd client** command in XR EXEC mode.

clear nsr ncd client {*PID value* | **all**} [**location** *node-id*]

Syntax Description

PID value	Process ID value of the client in which counters need to be cleared. The range is from 0 to 4294967295.
all	Clears the counters for all NCD clients.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The default value for the *node-id* argument is the current node in which the command is being executed. The *PID value* argument does not have a default value.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

The active and standby instances of some NSR-capable applications communicate through two queues, and these applications are multiplexed onto these queues. NSR consumer demuxer (NCD) is a process that provides the demuxing services on the receiver side.

You can use the **clear nsr ncd client** command to troubleshoot traffic issues. If you clear the existing counters, it can help you to monitor the delta changes.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear all the counters for all NCD clients:

```
RP/0/RP0/CPU0:router# clear nsr ncd client all
RP/0/RP0/CPU0:router# show nsr ncd client all

Client PID                          : 3874979
Client Protocol                     : TCP
Client Instance                     : 1
Total packets received              : 0
Total acks received                 : 0
Total packets/acks accepted         : 0
Errors in changing packet ownership  : 0
Errors in setting application offset : 0
Errors in enqueuing to client        : 0
Time of last clear                   : Sun Jun 10 14:43:44 20

RP/0/RP0/CPU0:router# show nsr ncd client brief

                             Total    Total   Accepted
Pid   Protocol   Instance    Packets Acks    Packets/Acks
3874979   TCP          1          0   0         0
```

clear nsr ncd queue

To clear the counters for the nonstop routing (NSR) Consumer Demuxer (NCD) queue, use the **clear nsr ncd queue** command in XR EXEC mode.

clear nsr ncd queue {**all** | **high** | **low**} [**location** *node-id*]

Syntax Description

all	Clears the counters for all the NCD queues.
high	Clears the counters for the high-priority NCD queue.
low	Clears the counters the low-priority NCD queue.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear the counters for all the NCD queues:

```
RP/0/RP0/CPU0:router# clear nsr ncd queue all
RP/0/RP0/CPU0:router# show nsr ncd queue all

Queue Name                           : NSR_LOW
Total packets received               : 0
Total packets accepted               : 0
Errors in getting datagram offset    : 0
Errors in getting packet length      : 0
Errors in calculating checksum       : 0
Errors due to bad checksum           : 0
Errors in reading packet data        : 0
Errors due to bad NCD header         : 0
Drops due to a non-existent client   : 0
Errors in changing packet ownership  : 0
Errors in setting application offset : 0
Errors in enqueuing to client        : 0
Time of last clear                   : Sun Jun 10 14:44:38 2007
```

```
Queue Name                           : NSR_HIGH
Total packets received               : 0
Total packets accepted               : 0
Errors in getting datagram offset    : 0
Errors in getting packet length      : 0
Errors in calculating checksum       : 0
Errors due to bad checksum           : 0
Errors in reading packet data        : 0
Errors due to bad NCD header         : 0
Drops due to a non-existent client   : 0
Errors in changing packet ownership  : 0
Errors in setting application offset : 0
Errors in enqueuing to client        : 0
Time of last clear                   : Sun Jun 10 14:44:38 2007

RP/0/RP0/CPU0:router# show nsr ncd queue brief

                          Total        Accepted
          Queue         Packets         Packets
        NSR_LOW               0               0
       NSR_HIGH               0               0
```

clear nsr npl

To clear NSR NPL wheel statistics for a given client and instance, use the **clear nsr npl** command in XR EXEC mode.

clear **nsr** **npl** **client** *client-name* **instance** *client-instance-number* **wheels**

[*wheel-ID* | [**location** *node-id*]]

Table 63: Syntax Description

npl	Clear NSR NPL wheel statistics for a given client and instanceas specified.
wheels	Displays client's wheel information.
wheel-id	(Optional) Displays client's wheel information with respect to the specified wheel-id.
location *node-id*	(Optional) Displays information for the designated node.

Command Default

The location defaults to the current node in which the command is executing.

Command Mode

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Though this command is used to clear NSR NPL statistics for a given client instance and/or for a given wheel id, this command can also be used for debugging purpose to measure delta.

Task ID

Task ID	Operations
transport	execute

Use the **show nsr npl client bgp instance 0 wheels** command for checking counters:

```
Router# show nsr npl client bgp instance 0 wheels
NPL wheel '1' information
-------------------------
Wheel initialized, wheel ID: 1
Total msgs sent: 13, total acks received: 13
Last sequence number: 26
Total msgs received: 6, total acks sent: 6

Retransmission information
--------------------------
```

```
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 1, Next expected seq: 7, Max limit: 30
Last ISN update time: 'May 11 18:57:46.452.333'
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0


NPL wheel '2' information
-------------------------
Wheel initialized, wheel ID: 2
Total msgs sent: 0, total acks received: 0
Last sequence number: 0
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 0, Next expected seq: 0, Max limit: 30
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0


NPL wheel '3' information
-------------------------
Wheel initialized, wheel ID: 3
Total msgs sent: 0, total acks received: 0
Last sequence number: 0
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 0, Next expected seq: 0, Max limit: 30
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0


NPL wheel '4' information
-------------------------
Wheel initialized, wheel ID: 4
Total msgs sent: 0, total acks received: 0
Last sequence number: 0
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0
```

```
Out of order information
------------------------
ISN: 0, Next expected seq: 0, Max limit: 30
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0
```

Use the **clear nsr npl client bgp instance 0 wheels** command to clear counters.

```
Router# clear nsr npl client bgp instance 0 wheels
```

Now, use the show nsr npl client bgp instance 0 wheels command again for checking counters. You can see the cleared counters highlighted.

```
Router# show nsr npl client bgp instance 0 wheels
NPL wheel '1' information
-------------------------
Wheel initialized, wheel ID: 1
Total msgs sent: 0, total acks received: 0
Last sequence number: 26
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 1, Next expected seq: 7, Max limit: 30
Last ISN update time: 'May 11 18:57:46.452.333'
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0


NPL wheel '2' information
-------------------------
Wheel initialized, wheel ID: 2
Total msgs sent: 0, total acks received: 0
Last sequence number: 0
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 0, Next expected seq: 0, Max limit: 30
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0


NPL wheel '3' information
-------------------------
Wheel initialized, wheel ID: 3
Total msgs sent: 0, total acks received: 0
Last sequence number: 0
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
```

```
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 0, Next expected seq: 0, Max limit: 30
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0


NPL wheel '4' information
-------------------------
Wheel initialized, wheel ID: 4
Total msgs sent: 0, total acks received: 0
Last sequence number: 0
Total msgs received: 0, total acks sent: 0

Retransmission information
--------------------------
Total msgs retransmitted: 0, timeouts: 0
Num of entries in the queue: 0

Out of order information
------------------------
ISN: 0, Next expected seq: 0, Max limit: 30
Total msgs reassembled: 0
Total msgs drops: 0
Num of entries in the queue: 0
```

clear raw statistics pcb

To clear statistics for a single RAW connection or for all RAW connections, use the **clear raw statistics pcb** command in XR EXEC mode.

clear raw statistics pcb {**all***pcb-address*} [**location***node-id*]

Syntax Description

all	Clears statistics for all RAW connections.
pcb-address	Clears statistics for a specific RAW connection.
location *node-id*	(Optional) Clears statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **all** keyword to clear all RAW connections. To clear a specific RAW connection, enter the protocol control block (PCB) address of the RAW connection. **Use the show raw brief** command to obtain the PCB address.

Use the **location** keyword and *node-id* argument to clear RAW statistics for a designated node.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear statistics for a RAW connection with PCB address 0x80553b0:

```
RP/0/RP0/CPU0:router# clear raw statistics pcb 0x80553b0
RP/0/RP0/CPU0:router# show raw statistics pcb 0x80553b0

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

The following example shows how to clear statistics for all RAW connections:

```
RP/0/RP0/CPU0:router# clear raw statistics pcb all
RP/0/RP0/CPU0:router# show raw statistics pcb all

Statistics for PCB 0x805484c
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application

Statistics for PCB 0x8054f80
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

clear tcp nsr client

To bring the nonstop routing (NSR) down on all the sessions that are owned by the specified client, use the **clear tcp nsr client** command in XR EXEC mode.

clear tcp nsr client {*ccb-address* | **all**} [**location** *node-id*]

Syntax Description

ccb-address	Client Control Block (CCB) of the NSR client.
all	Specifies all the clients.
location *node-id*	(Optional) Displays client information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

The location defaults to the current node in which the command is executing.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

The output of the **show tcp nsr client** command is used to locate the CCB of the desired client.

Use the **clear tcp nsr client** command to gracefully bring down NSR session that are owned by one client or all clients. In addition, the **clear tcp nsr client** command is used as a work around if the activity on the sessions freezes.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the nonstop routing (NSR) client is cleared for 0x482afacc. The two sessions had NSR already up before executing the **clear tcp nsr client** command. NSR is no longer up after executing the **clear tcp nsr client** command.

```
RP/0/RP0/CPU0:router# show tcp nsr client brief

CCB          Proc Name    Instance     Sets       Sessions/NSR Up Sessions
0x482c10e0   mpls_ldp          1            2          3/1
0x482afacc   mpls_ldp          2            1          2/2

RP/0/RP0/CPU0:router# clear tcp nsr client 0x482afacc
RP/0/RP0/CPU0:router# show tcp nsr client brief

CCB          Proc Name    Instance     Sets       Sessions/NSR Up Sessions
0x482c10e0   mpls_ldp          1            2          3/1
0x482afacc   mpls_ldp          2            1          2/0
```

clear tcp nsr pcb

To bring the nonstop routing (NSR) down on a specified connection or all connections, use the **clear tcp nsr pcb** command in XR EXEC mode.

clear tcp nsr pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	PCB address range for the specific connection information. 0 to ffffffff. For example, the address range can be 0x482a4e20.
all	Specifies all the connections.
location *node-id*	(Optional) Displays connection information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

The output of the **show tcp nsr brief** command is used to locate the Protocol Control Block (PCB) of a desired connection.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the information for TCP connections is cleared:

```
RP/0/RP0/CPU0:router# show tcp nsr brief

Wed Dec 2 20:35:47.467 PST
--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------
PCB                    VRF-ID   Local Address   Foreign Address NSR(US/DS)
0x00007f9e3c028538 0x60000000 3.3.3.3:646     5.5.5.5:17931    NA/Up
0x00007f9e3c021fb8 0x60000000 3.3.3.3:646     4.4.4.4:29301    NA/Up
0x00007f9e3c007248 0x60000000 3.3.3.3:646     12.1.105.2:32877 NA/Up
0x00007f9e3c010c78 0x60000000 3.3.3.3:646     6.6.6.6:56296    NA/Up
0x00007f9de4001798 0x60000000 3.3.3.3:12888   2.2.2.2:646      NA/Up
0x00007f9e3c04a338 0x60000000 3.3.3.13:179    2.2.2.13:13021   NA/Up
0x00007f9e3c026c78 0x60000000 3.3.3.3:179     4.4.4.4:15180    NA/Up
0x00007f9e3c019b38 0x60000000 3.3.3.3:179     8.8.8.8:21378    NA/Up
0x00007f9e3c029df8 0x60000000 3.3.3.22:179    2.2.2.22:24482   NA/Up
0x00007f9e3c064538 0x60000000 3.3.3.14:179    2.2.2.14:27569   NA/Up
```

```
0x00007f9e3c041008 0x60000000 3.3.3.25:179    2.2.2.25:29654   NA/Up

RP/0/RP0/CPU0:router# clear tcp nsr pcb 0x00007f9e3c028538
RP/0/RP0/CPU0:router# clear tcp nsr pcb 0x00007f9e3c021fb8
RP/0/RP0/CPU0:router# show tcp nsr brief

Wed Dec 2 20:35:47.467 PST
--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------
PCB                  VRF-ID   Local Address   Foreign Address NSR(US/DS)
0x00007f9e3c028538 0x60000000 3.3.3.3:646     5.5.5.5:17931    NA/Down
0x00007f9e3c021fb8 0x60000000 3.3.3.3:646     4.4.4.4:29301    NA/Down
0x00007f9e3c007248 0x60000000 3.3.3.3:646     12.1.105.2:32877 NA/Up
0x00007f9e3c010c78 0x60000000 3.3.3.3:646     6.6.6.6:56296    NA/Up
0x00007f9de4001798 0x60000000 3.3.3.3:12888   2.2.2.2:646      NA/Up
0x00007f9e3c04a338 0x60000000 3.3.3.13:179    2.2.2.13:13021   NA/Up
0x00007f9e3c026c78 0x60000000 3.3.3.3:179     4.4.4.4:15180    NA/Up
0x00007f9e3c019b38 0x60000000 3.3.3.3:179     8.8.8.8:21378    NA/Up
0x00007f9e3c029df8 0x60000000 3.3.3.22:179    2.2.2.22:24482   NA/Up
0x00007f9e3c064538 0x60000000 3.3.3.14:179    2.2.2.14:27569   NA/Up
0x00007f9e3c041008 0x60000000 3.3.3.25:179    2.2.2.25:29654   NA/Up
```

clear tcp nsr session-set

To clear the nonstop routing (NSR) on all the sessions in the specified session-set or all session sets, use the **clear tcp nsr session-set** command in XR EXEC mode.

clear tcp nsr session-set { *sscb-address* | **all**} [**location** *node-id*]

Syntax Description

sscb-address	Session-Set Control Block (SSCB) address range for the specific session set information. 0 to ffffffff. For example, the address range can be 0x482a4e20.
all	Specifies all the session sets.
location *node-id*	(Optional) Displays session set information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

The output of the **show tcp nsr session-set brief** command is used to locate the SSCB of the desired session-set.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the information for the session sets is cleared:

```
RP/0/RP0/CPU0:router# show tcp nsr client brief

CCB                Proc Name         Instance  Sets       Sessions/NSR Up Sessions
0x482b5ee0         mpls_ldp             1        1           10/10

RP/0/RP0/CPU0:router# clear tcp nsr client 0x482b5ee0
RP/0/RP0/CPU0:router# show tcp nsr client brief

CCB                Proc Name         Instance  Sets       Sessions/NSR Up Sessions
0x482b5ee0         mpls_ldp             1        1           10/0
```

clear tcp nsr statistics client

To clear the nonstop routing (NSR) statistics of the client, use the **clear tcp nsr statistics client** command in XR EXEC mode.

clear tcp nsr statistics client {*ccb-address* | **all**} [**location** *node-id*]

Syntax Description

ccb-address	Client Control Block (CCB) of the desired client. For example, the address range can be 0x482a4e20.
all	Specifies all the clients.
location *node-id*	(Optional) Displays client information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the statistics for the NSR clients is cleared:

```
Router# show tcp nsr statistics client all

--------------------------------------------------------------
                     Node: 0/0/CPU0
--------------------------------------------------------------

==============================================================
CCB: 0xed30cd58
Name: bgp, Job ID: 1085
Connected at: Mon May 11 17:29:20 2020

Notification Statistics :          Queued     Failed      Delivered    Dropped
Init-Sync Done          :         4        0          4        0
Replicated Session Ready:            0           0             0           0
Operational Down        :         3        0          3        0
Init-Sync Stop Reading  :         3        0          3        0
```

```
Last clear at: Never Cleared

Router# clear tcp nsr statistics client all

Riuter# show tcp nsr statistics client all

--------------------------------------------------------------
                     Node: 0/0/CPU0
--------------------------------------------------------------

==============================================================
CCB: 0xed30cd58
Name: bgp, Job ID: 1085
Connected at: Mon May 11 17:29:20 2020

Notification Statistics :         Queued     Failed  Delivered    Dropped
Init-Sync Done          :         0       0    0          0
Replicated Session Ready:            0          0       0             0
Operational Down        :         0       0    0          0
Init-Sync Stop Reading  :         0       0    0          0
Last clear at: Mon May 11 19:08:56 2020
```

clear tcp nsr statistics pcb

To clear the nonstop routing (NSR) statistics for TCP connections, use the **clear tcp nsr statistics pcb** command in XR EXEC mode.

clear tcp nsr statistics pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	PCB address range for the specific connection information. 0 to fffffff. For example, the address range can be 0x482a4e20.
all	Specifies all the connections.
location *node-id*	(Optional) Displays connection information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the NSR statistics for TCP connections is cleared:

```
RP/0/RP0/CPU0:router# show tcp nsr statistics pcb 0x482d14c8

===============================================================
PCB 0x482d14c8
Number of times NSR went up: 1
Number of times NSR went down: 0
Number of times NSR was disabled: 0
Number of times switch-over occured : 0
IACK RX Message Statistics:
        Number of iACKs dropped because SSO is not up               : 0
        Number of stale iACKs dropped                               : 1070
        Number of iACKs not held because of an immediate match      : 98
TX Messsage Statistics:
        Data transfer messages:
            Sent 317, Dropped 0, Data (Total/Avg.) 2282700/7200
            Rcvd 0
                Success           : 0
                Dropped (Trim)    : 0
        Segmentation instructions:
            Sent 1163, Dropped 0, Units (Total/Avg.) 4978/4
            Rcvd 0
                Success           : 0
                Dropped (Trim)    : 0
                Dropped (TCP)     : 0
        NACK messages:
            Sent 0, Dropped 0
            Rcvd 0
                Success           : 0
                Dropped (Data snd): 0
        Cleanup instructions      :
            Sent 8, Dropped 0
            Rcvd 0
                Success           : 0
                Dropped (Trim)    : 0
Last clear at: Never cleared

RP/0/RP0/CPU0:router# clear tcp nsr statistics pcb 0x482d14c8
RP/0/RP0/CPU0:router# show tcp nsr statistics pcb 0x482d14c8

==============================================================
PCB 0x482d14c8
Number of times NSR went up: 0
Number of times NSR went down: 0
Number of times NSR was disabled: 0
Number of times switch-over occured : 0
IACK RX Message Statistics:
        Number of iACKs dropped because SSO is not up               : 0
        Number of stale iACKs dropped                               : 0
        Number of iACKs not held because of an immediate match      : 0
TX Messsage Statistics:
        Data transfer messages:
            Sent 0, Dropped 0, Data (Total/Avg.) 0/0
            Rcvd 0
                Success           : 0
                Dropped (Trim)    : 0
        Segmentation instructions:
            Sent 0, Dropped 0, Units (Total/Avg.) 0/0
            Rcvd 0
                Success           : 0
                Dropped (Trim)    : 0
                Dropped (TCP)     : 0
        NACK messages:
            Sent 0, Dropped 0
            Rcvd 0
                Success           : 0
                Dropped (Data snd): 0
        Cleanup instructions      :
            Sent 0, Dropped 0
            Rcvd 0
                Success           : 0
                Dropped (Trim)    : 0
Last clear at: Thu Aug 16 18:32:12 2007
```

clear tcp nsr statistics session-set

To clear the nonstop routing (NSR) statistics for session sets, use the **clear tcp nsr statistics session-set** command in XR EXEC mode mode.

clear tcp nsr statistics session-set {*sscb-address* | **all**} [**location** *node-id*]

Syntax Description

sscb-address	Session-Set Control Block (SSCB) address range for the specific session set information. 0 to ffffffff. For example, the address range can be 0x482a4e20.
all	Specifies all the session sets.
location *node-id*	(Optional) Displays session set information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the NSR statistics for session sets is cleared:

```
RP/0/RP0/CPU0:router# show tcp nsr statistics session-set all

===================Session Set Stats ===========================
SSCB 0x482b6684, Set ID: 1
Number of times init-sync was attempted  :3
Number of times init-sync was successful :3
Number of times init-sync failed         :0
Number of times switch-over occured      :0
Last clear at: Never Cleared

RP/0/RP0/CPU0:router# clear tcp nsr statistics session-set all
RP/0/RP0/CPU0:router# show tcp nsr statistics session-set all

===================Session Set Stats ===========================
SSCB 0x482b6684, Set ID: 1
Number of times init-sync was attempted  :0
Number of times init-sync was successful :0
Number of times init-sync failed         :0
Number of times switch-over occured      :0
Last clear at: Thu Aug 16 18:37:00 2007
```

clear tcp nsr statistics summary

To clear the nonstop routing (NSR) statistics summary, use the **clear tcp nsr statistics summary** command in XR EXEC mode.

clear tcp nsr statistics summary [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays statistics summary information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear the summary statistics:

```
Router# show tcp nsr statistics client all

--------------------------------------------------------------
                     Node: 0/0/CPU0
--------------------------------------------------------------

==============================================================
CCB: 0xed30cd58
Name: bgp, Job ID: 1085
Connected at: Mon May 11 17:29:20 2020

Notification Statistics :      Queued     Failed  Delivered    Dropped
Init-Sync Done          :      4       0    4          0
Replicated Session Ready:         0          0       0             0
Operational Down        :      3       0    3          0
Init-Sync Stop Reading  :      3       0    3          0
Last clear at: Never Cleared

Router# clear tcp nsr statistics client all

Router# show tcp nsr statistics client all

--------------------------------------------------------------
                     Node: 0/0/CPU0
--------------------------------------------------------------
```

```
==============================================================
CCB: 0xed30cd58
Name: bgp, Job ID: 1085
Connected at: Mon May 11 17:29:20 2020

Notification Statistics :      Queued     Failed  Delivered    Dropped
Init-Sync Done          :      0       0    0          0
Replicated Session Ready:         0          0       0             0
Operational Down        :      0       0    0          0
Init-Sync Stop Reading  :      0       0    0          0
Last clear at: Mon May 11 19:08:56 2020
```

clear tcp pcb

To clear TCP protocol control block (PCB) connections, use the **clear tcp pcb** command in XR EXEC mode.

clear tcp pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	Clears the TCP connection at the specified PCB address.
all	Clears all open TCP connections.
location *node-id*	(Optional) Clears the TCP connection for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **clear tcp pcb** command is useful for clearing hung TCP connections. Use the `show tcp brief` command to find the PCB address of the connection you want to clear.

If the **clear tcp pcb all** command is used, the software does not clear a TCP connection that is in the listen state. If a specific PCB address is specified, then a connection in listen state is cleared.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the TCP connection at PCB address 0x00007f7da4007eb8 is cleared:

```
Router# show tcp brief

PCB                       VRF-ID      Recv-Q Send-Q Local Address          Foreign Address
        State
0x00007f7d4c011d38        0x60000000        0      0     :::22                  :::0
           LISTEN
0x00007f7d4c00cf68        0x00000000        0      0     :::22                  :::0
           LISTEN
0x00007f7d4c00c6a8        0x60000000        0      0     :::179                 :::0
           LISTEN
0x00007f7d4c007db8        0x00000000        0      0     :::179                 :::0
           LISTEN
0x00007f7d7003fab8        0x60000000        0      0     :::0                   :::0
           CLOSED
0x00007f7d7003afa8        0x00000000        0      0     :::0                   :::0
           CLOSED
```

```
0x00007f7d4c035378       0x60000000       0     0     133.1.2.2:25032       133.1.2.1:179
        ESTAB
0x00007f7da4007eb8  0x60000000       0      0     10.86.188.84:179      10.86.188.99:28148
   ESTAB
0x00007f7d700405e8        0x60000000        0      0     32.32.32.32:54157
149.127.13.12:57000  SYNSENT
0x00007f7da400cfe8        0x60000000        0      0     10.86.188.84:23
173.39.52.160:60586  ESTAB
0x00007f7d4c011aa8        0x60000000        0      0     0.0.0.0:22             0.0.0.0:0
           LISTEN
0x00007f7d70030218        0x00000000        0      0     0.0.0.0:22             0.0.0.0:0
           LISTEN
0x00007f7d70021da8        0x60000000        0      0     0.0.0.0:23             0.0.0.0:0
           LISTEN
0x00007f7d4c006858        0x60000002        0      0     0.0.0.0:23             0.0.0.0:0
           LISTEN
0x00007f7d4c000fd8        0x00000000        0      0     0.0.0.0:23             0.0.0.0:0
           LISTEN
0x00007f7d7003a858        0x60000000        0      0     0.0.0.0:646            0.0.0.0:0
           LISTEN
0x00007f7d70035cd8        0x00000000        0      0     0.0.0.0:646            0.0.0.0:0
           LISTEN
0x00007f7d7002fa08        0x60000000        0      0     0.0.0.0:179            0.0.0.0:0
           LISTEN
0x00007f7d70028b28        0x00000000        0      0     0.0.0.0:179            0.0.0.0:0
           LISTEN
0x00007f7d70023188        0x00000000        0      0     0.0.0.0:0              0.0.0.0:0
           CLOSED

Router# clear tcp pcb 0x00007f7da4007eb8

Router# show tcp brief

   PCB                     VRF-ID      Recv-Q Send-Q Local Address         Foreign Address
        State
0x00007f7d4c011d38         0x60000000      0      0      :::22                  :::0
             LISTEN
0x00007f7d4c00cf68         0x00000000      0      0      :::22                  :::0
             LISTEN
0x00007f7d4c00c6a8         0x60000000      0      0      :::179                 :::0
             LISTEN
0x00007f7d4c007db8         0x00000000      0      0      :::179                 :::0
             LISTEN
0x00007f7d7003fab8         0x60000000      0      0      :::0                   :::0
             CLOSED
0x00007f7d7003afa8         0x00000000      0      0      :::0                   :::0
             CLOSED
0x00007f7d4c035378   0x60000000      0      0      133.1.2.2:25032        133.1.2.1:179
       ESTAB
0x00007f7da400cfe8   0x60000000     0      0     10.86.188.84:23       173.39.52.160:60586
    ESTAB
0x00007f7d4c011aa8         0x60000000      0      0      0.0.0.0:22             0.0.0.0:0
             LISTEN
0x00007f7d70030218         0x00000000      0      0      0.0.0.0:22             0.0.0.0:0
             LISTEN
0x00007f7d70021da8         0x60000000      0      0      0.0.0.0:23             0.0.0.0:0
             LISTEN
0x00007f7d4c006858         0x60000002      0      0      0.0.0.0:23             0.0.0.0:0
             LISTEN
0x00007f7d4c000fd8         0x00000000      0      0      0.0.0.0:23             0.0.0.0:0
             LISTEN
0x00007f7d7003a858         0x60000000      0      0      0.0.0.0:646            0.0.0.0:0
             LISTEN
0x00007f7d70035cd8         0x00000000      0      0      0.0.0.0:646            0.0.0.0:0
```

```
            LISTEN
0x00007f7d7002fa08          0x60000000      0      0      0.0.0.0:179            0.0.0.0:0
            LISTEN
0x00007f7d70028b28          0x00000000      0      0      0.0.0.0:179            0.0.0.0:0
            LISTEN
0x00007f7d70023188          0x00000000      0      0      0.0.0.0:0              0.0.0.0:0
            CLOSED
```

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in

XR EXEC mode.

clear tcp statistics { **client** | **pcb** { **all** | *pcb-address* } | **summary**} **location** *node-id*

Syntax Description

client	(Optional) Clears statistics for all TCP clients.
pcb all	(Optional) Clears statistics for all TCP connections.
pcb *pcb-address*	Clears statistics for a specific TCP connection.
summary	Clears summary statistic for a specific node or connection.
location *node-id*	Clears TCP statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Though this command is used to clear incoming and outgoing TCP packet statiscs of all clients of given location, PCB, and summary statistics; this command can be used for debugging purpose to measure delta.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows that the statistics for the NSR clients is cleared:

```
Router# show tcp statistics client

Name     JID            IPv4-Stats                    IPv6-Stats
                   Sent-Packets Recv-Packets   Sent-Packets Recv-Packets
igmp     1151       5            9             0            3
mld      1156       9            4             4            0
pim      1157       8            3             5            2
pim6     1158       9            4             6            1
Router# clear tcp tatistics client

Riuter# show nsr statistics client


Name     JID            IPv4-Stats                    IPv6-Stats
                   Sent-Packets Recv-Packets   Sent-Packets Recv-Packets
```

```
igmp     1151       0             0               0             0
mld      1156       0             0               0             0
pim      1157       0             0               0             0
pim6     1158       0             0               0             0
```

clear udp statistics

To clear User Datagram Protocol (UDP) statistics, use the **clear udp statistics** command in

XR EXEC mode.

clear udp statistics { **client** | **pcb** { **all** | *pcb-address* } | **summary** } **location** *node-id*

Syntax Description

client	(Optional) Clears statistics for all TCP clients.
pcb all	Clears statistics for all UDP connections.
pcb *pcb-address*	Clears statistics for a specific UDP connection.
summary	Clears UDP summary statistics.
location *node-id*	(Optional) Clears UDP statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Though this command is used to clear incoming and outgoing TCP packet statiscs of all clients of given location, PCB, and summary statistics; this command can be used for debugging purpose to measure delta.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear UDP summary statistics:

```
Router# show udp statistics summary
UDP statistics:
Rcvd: 121 Total, 121 drop, 0 no port
      0 checksum error, 0 too short
Sent: 121 Total, 0 error
0 Total forwarding broadcast packets
0 Cloned packets, 0 failed cloning

Router# clear udp statistics summary

Router# show udp statistics summary
UDP statistics:
Rcvd: 9 Total, 9 drop, 0 no port
      0 checksum error, 0 too short
Sent: 9 Total, 0 error
```

```
0 Total forwarding broadcast packets
0 Cloned packets, 0 failed cloning
```

forward-protocol udp

To configure the system to forward any User Datagram Protocol (UDP) datagrams that are received as broadcast packets to a specified helper address, use the **forward-protocol udp** command in

XR Config mode.

To restore the system to its default condition with respect to this command, use the **no** form of this command.

forward-protocol udp {*port-number* | **disable** | **domain** | **nameserver** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp**}
no forward-protocol udp {*port-number* | **disable** | **domain** | **nameserver** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp**}

Syntax Description

port-number	Forwards UDP broadcast packets to a specified port number. Range is 1 to 65535.
disable	Disables IP Forward Protocol UDP.
domain	Forwards UDP broadcast packets to Domain Name Service (DNS, 53).
nameserver	Forwards UDP broadcast packets to IEN116 name service (obsolete, 42).
netbios-dgm	Forwards UDP broadcast packets to NetBIOS datagram service (138).
netbios-ns	Forwards UDP broadcast packets to NetBIOS name service (137).
tacacs	Forwards UDP broadcast packets to TACACS (49).
tftp	Forwards UDP broadcast packets to TFTP (69).

Command Default

forward-protocol udp is enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **forward-protocol udp** command to specify that UDP broadcast packets received on the incoming interface are forwarded to a specified helper address.

When you configure the **forward-protocol udp** command, you must also configure the **helper-address** command to specify a helper address on an interface. The helper address is the IP address to which the UDP datagram is forwarded. Configure the **helper-address** command with IP addresses of hosts or networking devices that can handle the service. Because the helper address is configured per interface, you must configure a helper address for each incoming interface that will be receiving broadcasts that you want to forward.

You must configure one **forward-protocol udp** command per UDP port you want to forward. The port on the packet is either port 53 (**domain**), port 69 (**tftp**), or a port number you specify.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to specify that all UDP broadcast packets with port 53 or port 69 received on incoming HundredGigE interface 0/RP0/CPU0 are forwarded to 172.16.0.1. HundredGigE interface 0/RP0/CPU0 receiving the UDP broadcasts is configured with a helper address of 172.16.0.1, the destination address to which the UDP datagrams are forwarded.

```
RP/0/RP0/CPU0:router(config)# forward-protocol udp domain disable
RP/0/RP0/CPU0:router(config)# forward-protocol udp tftp disable
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/RP0/CPU0
RP/0/RP0/CPU0:router(config-if)# ipv4 helper-address 172.16.0.1
```

nsr process-failures switchover

To configure failover as a recovery action for active instances to switch over to a standby route processor (RP) or a standby distributed route processor (DRP) to maintain nonstop routing (NSR), use the **nsr process-failures switchover** command in XR Config mode. To disable this feature, use the **no** form of this command.

nsr process-failures switchover
no nsr process-failures switchover

Syntax Description

This command has no keywords or arguments.

Command Default

If not configured, a process failure of the active TCP or its applications (for example LDP, BGP, and so forth) can cause sessions to go down, and NSR is not provided.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to use the **nsr process-failures switchover** command:

```
RP/0/RP0/CPU0:router(config)# nsr process-failures switchover
```

service tcp-small-servers

To enable small TCP servers such as the ECHO, use the **service tcp-small-servers** command in XR Config mode. To disable the TCP server, use the **no** form of this command.

service {**ipv4** | **ipv6**} **tcp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]
no service {**ipv4** | **ipv6**} **tcp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]

Syntax Description

ip4	Specifies IPv4 small servers.
ipv6	Specifies IPv6 small servers.
max-servers	(Optional) Sets the number of allowable TCP small servers.
number	(Optional) Number value. Range is 1 to 2147483647.
no-limit	(Optional) Sets no limit to the number of allowable TCP small servers.
access-list-name	(Optional) The name of an access list.

Command Default

TCP small servers are disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The TCP small servers currently consist of three services: Discard (port 9), Echo (port 7), and Chargen (port 19). These services are used to test the TCP transport functionality. The Discard server receives data and discards it. The Echo server receives data and echoes the same data to the sending host. The Chargen server generates a sequence of data and sends it to the remote host.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

Examples

In the following example, small IPv4 TCP servers are enabled:

```
RP/0/RP0/CPU0:router(config)# service ipv4 tcp-small-servers max-servers 5 acl100
```

service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the ECHO, use the **service udp-small-servers** command in XR Config mode. To disable the UDP server, use the **no** form of this command.

service {**ipv4** | **ipv6**} **udp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]
no service {**ipv4** | **ipv6**} **udp-small-servers** [**max-servers** *number* | **no-limit**] [*access-list-name*]

Syntax Description

ip4	Specifies IPv4 small servers.
ipv6	Specifies IPv6 small servers.
max-servers	(Optional) Sets the number of allowable UDP small servers.
number	(Optional) Number value. Range is 1 to 2147483647.
no-limit	(Optional) Sets no limit to the number of allowable UDP small servers.
access-list-name	(Optional) Name of an access list.

Command Default

UDP small servers are disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The UDP small servers currently consist of three services: Discard (port 9), Echo (port 7), and Chargen (port 19). These services are used to test the UDP transport functionality. The discard server receives data and discards it. The echo server receives data and echoes the same data to the sending host. The chargen server generates a sequence of data and sends it to the remote host.

Task ID

Task ID	Operations
ipv6	read, write
ip-services	read, write

Examples

The following example shows how to enable small IPv6 UDP servers and set the maximum number of allowable small servers to 10:

```
RP/0/RP0/CPU0:router(config)# service ipv6 udp-small-servers max-servers 10
```

show nsr ncd client

To display information about the clients for nonstop routing (NSR) Consumer Demuxer (NCD), use the **show nsr ncd client** command in XR EXEC mode.

show nsr ncd client {*PID value* | **all** | **brief**} [**location** *node-id*]

Syntax Description

PID v alue	Process ID (PID) information for a specific client. The range is from 0 to 4294967295.
all	Displays detailed information about all the clients.
brief	Displays brief information about all the clients.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows detailed information about all the clients:

```
RP/0/RP0/CPU0:router# show nsr ncd client all

Client PID                          : 3874979
Client Protocol                     : TCP
Client Instance                     : 1
Total packets received              : 28
Total acks received                 : 0
Total packets/acks accepted         : 28
Errors in changing packet ownership  : 0
Errors in setting application offset : 0
Errors in enqueuing to client       : 0
Time of last clear                  : Never cleared
```

The following sample output shows brief information about all the clients:

```
RP/0/RP0/CPU0:router# show nsr ncd client brief
```

```
                              Total   Total    Accepted
Pid   Protocol   Instance     Packets Acks     Packets/Acks
3874979   TCP          1          28  0               28
```

This table describes the significant fields shown in the display.

Table 64: show nsr ncd client Command Field Descriptions

Field	Description
Client PID	Process ID of the client process.
Client Protocol	Protocol of the client process. The protocol can be either TCP, OSPF, or BGP.
Client Instance	Instance number of the client process. There can be more than one instance of a routing protocol, such as OSPF.
Total packets received	Total packets received from the partner stack on the partner route processor (RP).
Total acks received	Total acknowledgements received from the partner stack on the partner RP for the packets sent to the partner stack.
Total packets/acks accepted	Total packets and acknowledgements received from the partner stack on the partner RP.
Errors in changing packet ownership	NCD changes the ownership of the packet to that of the client before queueing the packet to the client. This counter tracks the errors, if any, in changing the ownership.
Errors in setting application offset	NCD sets the offset of the application data in the packet before queueing the packet to the client. This counter tracks the errors, if any, in setting this offset.
Errors in enqueuing to client	Counter tracks any queueing errors.
Time of last clear	Statistics last cleared by the user.

show nsr ncd queue

To display information about the queues that are used by the nonstop routing (NSR) applications to communicate with their partner stacks on the partner route processors (RPs), use the **show nsr ncd queue** command in XR EXEC mode.

show nsr ncd queue {**all** | **brief** | **high** | **low**} [**location** *node-id*]

Syntax Description

all	Displays detailed information about all the consumer queues.
brief	Displays brief information about all the consumer queues.
high	Displays information about high-priority Queue and Dispatch (QAD) queues.
low	Displays information about low-priority QAD queues.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows brief information about all the consumer queues:

```
RP/0/RP0/CPU0:router# show nsr ncd queue brief

                           Total        Accepted
            Queue        Packets         Packets
          NSR_LOW            992             992
         NSR_HIGH              0               0
```

This table describes the significant fields shown in the display.

Table 65: show nsr ncd queue Command Field Descriptions

Field	Description
Total Packets	Total number of packets that are received from the partner stack.

Field	Description
Accepted Packets	Number of received packets that were accepted after performing some validation tasks.
Queue	Name of queue. NSR_HIGH and NSR_LOW are the two queues. High priority packets flow on the NSR_HIGH queue. Low priority packets flow on the NSR_LOW queue.

show raw brief

To display information about active RAW IP sockets, use the **show raw brief** command in XR EXEC mode.

show raw brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Protocols such as Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) use long-lived RAW IP sockets. The **ping** and **traceroute** commands use short-lived RAW IP sockets. Use the **show raw brief** command if you suspect a problem with one of these protocols.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show raw brief** command:

```
RP/0/RP0/CPU0:router# show raw brief

PCB      Recv-Q Send-Q Local Address         Foreign Address Protocol
0x805188c        0      0 0.0.0.0              0.0.0.0           2
0x8051dc8        0      0 0.0.0.0              0.0.0.0         103
0x8052250        0      0 0.0.0.0              0.0.0.0         255
```

This table describes the significant fields shown in the display.

Table 66: show raw brief Command Field Descriptions

Field	Description
PCB	Protocol control block address. This is the address to a structure that contains connection information such as local address, foreign address, local port, foreign port, and so on.
Recv-Q	Number of bytes in the receive queue.
Send-Q	Number of bytes in the send queue.
Local Address	Local address and local port.

Field	Description
Foreign Address	Foreign address and foreign port.
Protocol	Protocol that is using the RAW IP socket. For example, the number 2 is IGMP, 103 is PIM, and 89 is OSPF.

show raw detail pcb

To display detailed information about active RAW IP sockets, use the **show raw detail pcb** command in XR EXEC mode.

show raw detail pcb {*pcb-address* | **all**} **location** *node-id*

Syntax Description

pcb-address	Displays statistics for a specified RAW connection.
all	Displays statistics for all RAW connections.
location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show raw detail pcb** command displays detailed information for all connections that use the RAW transport. Information that is displayed includes family type (for example, 2 for AF_INET also known as IPv4), PCB address, Layer 4 (also known as transport) protocol, local address, foreign address, and any filter that is being used.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show raw detail pcb** command:

```
RP/0/RP0/CPU0:router# show raw detail pcb 0x807e89c

==============================================================
PCB is 0x807e89c, Family: 2, PROTO: 89
 Local host: 0.0.0.0
 Foreign host: 0.0.0.0

Current send queue size: 0
Current receive queue size: 0
Paw socket: Yes
```

This table describes the significant fields shown in the display.

Table 67: show raw detail pcb Command Field Descriptions

Field	Description
JID	Job ID of the process that created the socket.
Family	Network protocol. IPv4 is 2; IPv6 is 26.
PCB	Protocol control block address.
L4-proto	Layer 4 (also known as transport) protocol.
Laddr	Local address.
Faddr	Foreign address.
ICMP error filter mask	If an ICMP filter is being set, output in this field has a nonzero value.
LPTS socket options	If an LPTS option is being set, output in this field has a nonzero value.
Packet Type Filters	Packet filters that are being set for a particular RAW socket, including the number of packets for that filter type. Multiple filters can be set.

show raw extended-filters

To display information about active RAW IP sockets, use the **show raw extended-filters** command in XR EXEC mode.

show raw extended-filters {**interface-filter location** *node-id* | **location** *node-id* | **paktype-filter location** *node-id*}

Syntax Description

interface-filter	Displays the protocol control blocks (PCBs) with configured interface filters.
location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
paktype-filter	Displays the PCBs with configured packet type filters.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **show raw extended-filters** command displays detailed information for all connections that use the RAW transport. Information that is displayed includes family type (for example, 2 for AF_INET also known as IPv4), PCB address, Layer 4 (also known as transport) protocol, local address, foreign address, and any filter that is being used.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show raw extended-filters** command:

```
RP/0/RP0/CPU0:router# show raw extended-filters location 0/RP0/CPU0

Wed Dec 2 20:50:58.389 PST
-----------------------------------
JID: 1102
Family: 10
VRF: 0x60000000
PCB: 0x7fc4c4001f18
L4-proto: 255
Lport: 0
Fport: 0
```

This table describes the significant fields shown in the display.

Table 68: show raw extended-filters Output Command Field Descriptions

Field	Description
JID	Job ID of the process that created the socket.
Family	Network protocol. IPv4 is 2; IPv6 is 26.
PCB	Protocol control block address.
L4-proto	Layer 4 (also known as transport) protocol.
Laddr	Local address.
Faddr	Foreign address.
ICMP error filter mask	If an ICMP filter is being set, output in this field has a nonzero value.
LPTS socket options	If an LPTS option is being set, output in this field has a nonzero value.
Packet Type Filters	Packet filters that are being set for a particular RAW socket, including the number of packets for that filter type. Multiple filters can be set.

show raw statistics

To display statistics for a single RAW connection or for all RAW clients or connections, use the **show raw statistics pcb** command in XR EXEC mode.

show raw statistics { [| **pcb** | { **all** | *pcb-connection* }] | [| **clients** | { **location** *node-id* }] }

Syntax Description

clients	Displays statistics for all RAW clients.
pcb-address	Displays statistics for a specified RAW connection.
all	Displays statistics for all the clients.
location *node-id*	Displays RAW statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show raw statistics pcb all** command to display all RAW connections. If a specific RAW connection is desired, then enter the protocol control block (PCB) address of that RAW connection. Use the **show raw brief** command to obtain the PCB address.

Use the **location** keyword and *node-id* argument to display RAW statistics for a designated node.

Use the **show raw statistics pcb clients**This command is used to display incoming and outgoing (IPv4 and IPv6) packet statistics of RAW clients

Task ID

Task ID	Operations
transport	read

Examples

In the following example, statistics for a RAW connection with PCB address 0x80553b0 are displayed:

```
Router# show raw statistics pcb 0x80553b0

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
```

```
0 packets failed queued to application
```

In the following example, statistics for all RAW connections are displayed:

```
Router# show raw statistics pcb all

Statistics for PCB 0x805484c
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

In the following example, statistics for all RAW clients are displayed:

```
Router# show raw statistics clients location 0/RP0/CPU0

  Name        JID             IPv4-Stats                  IPv6-Stats
                      Sent-Packets  Recv-Packets  Sent-Packets  Recv-Packets
  igmp       1151           0             0             0             0
  mld        1156           0             0             0             0
  pim        1157           0             0             0             0
  pim6       1158           0             0             0             0
```

This table describes the significant fields shown in the display.

Table 69: show raw statistics pcb Command Field Descriptions

Field	Description
Send:	Statistics in this section refer to packets sent from an application to RAW.
Vrfid	VPN routing and forwarding (VRF) identification (vrfid) number.
xipc pulse received from application	Number of notifications sent from applications to RAW.
packets sent to network	Number of packets sent to the network.
packets failed getting queued to network	Number of packets that failed to get queued to the network.
Rcvd:	Statistics in this section refer to packets received from the network.
packets queued to application	Number of packets queued to an application.
packets failed queued to application	Number of packets that failed to get queued to an application.

show tcp brief

To display a summary of the TCP connection table, use the **show tcp brief** command in XR EXEC mode.

show tcp brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp brief** command:

```
Router# show tcp brief

TCPCB      Recv-Q Send-Q  Local Address           Foreign Address         State
0x80572a8       0      0  0.0.0.0:513             0.0.0.0:0               LISTEN
0x8056948       0      0  0.0.0.0:23              0.0.0.0:0               LISTEN
0x8057b60       0      3  10.8.8.2:23             10.8.8.1:1025           ESTAB
```

This table describes the significant fields shown in the display.

Table 70: show tcp brief Command Field Descriptions

Field	Description
TCPCB	Memory address of the TCP control block.
Recv-Q	Number of bytes waiting to be read.
Send-Q	Number of bytes waiting to be sent.
Local Address	Source address and port number of the packet.
Foreign Address	Destination address and port number of the packet.

Field	Description
State	State of the TCP connection.

show tcp detail

To display the details of the TCP connection table, use the **show tcp detail** command in XR EXEC mode.

show tcp detail pcb [*value* | **all**]

Syntax Description

pcb	Displays TCP connection information.
value	Displays a specific connection information. Range is from 0 to ffffffff.
all	Displays all connections information.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp detail pcb all** command:

```
Router# show tcp detail pcb all location 0/RP0/CPU0

Wed Dec 2 20:52:40.256 PST

==============================================================
Connection state is ESTAB, I/O status: 0, socket status: 0
Established at Wed Dec 2 20:25:42 2015

PCB 0x7f9dec013cc8, SO 0x7f9dec013858, TCPCB 0x7f9dec013f28, vrfid 0x60000000,
Pak Prio: Medium, TOS: 192, TTL: 1, Hash index: 506
Local host: 2011:1:120::1, Local port: 25093 (Local App PID: 5714)
Foreign host: 2011:1:120::2, Foreign port: 179

Current send queue size in bytes: 0 (max 24576)
Current receive queue size in bytes: 0 (max 32768) mis-ordered: 0 bytes
Current receive queue size in packets: 0 (max 0)

Timer      Starts   Wakeups   Next(msec)
Retrans     193       60        0
Sendwind     0        0         0
```

show tcp dump-file

To display the details of the PCB state from a dump file , use the **show tcp dump-file** command in XR EXEC mode.

show tcp dump-file { *dump-file-name* | | **all** | | **list** | { *ipv4-address-of-dumpfiles* | *ipv6-address-of-dumpfiles* | | **all** } } { **location** *node-id* }

Syntax Description

all	Displays all connections information.
location *node-id*	Displays RAW statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Although the basic use of this command is to provide information about list of all TCP dump files, details of a specific or all TCP dumpfile files, you can also use this command can be used for debugging purpose or to monitor flow of TCP packets for a TCP connection.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp dumpfile all location 0/RP0/CPU0** command:

```
Router# show tcp dumpfile list all location 0/RP0/CPU0

total 4
-rw-r--r-- 1 rpathark eng 3884 May 11 20:16 80_80_80_80.26355.179.cl.15892
```

show tcp extended-filters

To display the details of the TCP extended-filters, use the **show tcp extended-filters** command in XR EXEC mode.

show tcp extended-filters [**location** *node-id*]
peer-filter [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
peer-filter	(Optional) Displays connections with peer filter configured.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp extended-filters** command for a specific location (0/RP0/CPU0):

```
RP/0/RP0/CPU0:router# show tcp extended-filters location 0/RP0/CPU0

Total Number of matching PCB's in database: 3
-----------------------------------
JID: 135
Family: 2
PCB: 0x4826c5dc
L4-proto: 6
Lport: 23
Fport: 0
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x12

Flow Type: n/s
-----------------------------------

-----------------------------------
JID: 135
Family: 2
```

```
PCB: 0x4826dd8c
L4-proto: 6
Lport: 23
Fport: 59162
Laddr: 12.31.22.10
Faddr: 223.255.254.254
ICMP error filter mask: 0x12

Flow Type: n/s
-----------------------------------

-----------------------------------
JID: 135
Family: 2
PCB: 0x4826cac0
L4-proto: 6
Lport: 23
Fport: 59307
Laddr: 12.31.22.10
Faddr: 223.255.254.254
ICMP error filter mask: 0x12

Flow Type: n/s
-----------------------------------
```

show tcp nsr brief

To display the key nonstop routing (NSR) state of TCP connections on different nodes, use the **show tcp nsr brief** command in XR EXEC mode.

show tcp nsr brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for all TCP sessions for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows the administrative and operational NSR state of each TCP session in the NSR column:

```
RP/0/RP0/CPU0:router# show tcp nsr brief

Wed Dec 2 20:35:47.467 PST
--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------
PCB                  VRF-ID   Local Address   Foreign Address NSR(US/DS)
0x00007f9e3c028538 0x60000000 3.3.3.3:646     5.5.5.5:17931    NA/Up
0x00007f9e3c021fb8 0x60000000 3.3.3.3:646     4.4.4.4:29301    NA/Up
0x00007f9e3c007248 0x60000000 3.3.3.3:646     12.1.105.2:32877 NA/Up
0x00007f9e3c010c78 0x60000000 3.3.3.3:646     6.6.6.6:56296    NA/Up
0x00007f9de4001798 0x60000000 3.3.3.3:12888   2.2.2.2:646      NA/Up
0x00007f9e3c04a338 0x60000000 3.3.3.13:179    2.2.2.13:13021   NA/Up
0x00007f9e3c026c78 0x60000000 3.3.3.3:179     4.4.4.4:15180    NA/Up
0x00007f9e3c019b38 0x60000000 3.3.3.3:179     8.8.8.8:21378    NA/Up
0x00007f9e3c029df8 0x60000000 3.3.3.22:179    2.2.2.22:24482   NA/Up
0x00007f9e3c064538 0x60000000 3.3.3.14:179    2.2.2.14:27569   NA/Up
0x00007f9e3c041008 0x60000000 3.3.3.25:179    2.2.2.25:29654   NA/Up
```

This table describes the significant fields shown in the display.

Table 71: show tcp nsr brief Command Field Descriptions

Field	Description
PCB	Protocol Control Block (PCB).
Local Address	Local address and port of the TCP connection.
Foreign Address	Foreign address and port of the TCP connection.
NSR	Current operational NSR state of this TCP connection.
RevOnly	If yes, the TCP connection is replicated only in the receive direction. Some applications may need to replicate a TCP connection that is only in the receive direction.

show tcp nsr client brief

To display brief information about the state of nonstop routing (NSR) for TCP clients on different nodes, use the **show tcp nsr client brief** command in XR EXEC mode.

show tcp nsr client brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays brief client information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output is from the **show tcp nsr client brief** command:

```
RP/0/RP0/CPU0:router# show tcp nsr client brief location 0/1/CPU0


CCB          Proc Name     Instance Sets Sessions/NSR Up Sessions
0x482bf378   mpls_ldp  1        1             1/1
0x482bd32c   mpls_ldp  2        1             0/0
```

This table describes the significant fields shown in the display.

Table 72: show tcp nsr client brief Command Field Descriptions

Field	Description
CCB	Client Control Block (CCB). Unique ID to identify the client.
Proc Name	Name of the client process.
Instance	Instance is identified as the instance number of the client process because there can be more than one instance for a routing application.
Sets	Set number is identified as the ID of the session-set.
Sessions/NSR Up Sessions	Total sessions in the set versus the number of the sessions in which NSR is up.

show tcp nsr detail client

To display detailed information about the nonstop routing (NSR) clients, use the **show tcp nsr detail client** command in XR EXEC mode.

show tcp nsr detail client {*ccb-address* | **all**} [**location** *node-id*]

Syntax Description

ccb-address	Client Control Block (CCB) address range for the specific client information. 0 to ffffffff. For example, the address range can be 0x482a4e20.
all	Displays nonstop routing (NSR) details all the clients.
location *node-id*	(Optional) Displays client information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows detailed information for all clients:

```
Router# show tcp nsr detail client all


============================================================
CCB 0x482b25d8, Proc Name mpls_ldp
Instance ID 1, Job ID 360
Number of session-sets 2
Number of sessions 3
Number of NSR Synced sessions 1
Connected at: Sun Jun 10 07:05:31 2007
Registered for notifications: Yes

============================================================
CCB 0x4827fd30, Proc Name mpls_ldp
Instance ID 2, Job ID 361
Number of session-sets 1
Number of sessions 2
Number of NSR Synced sessions 2
Connected at: Sun Jun 10 07:05:54 2007
Registered for notifications: Yes
```

```
============================================================

Router# show tcp nsr detail client all location 1
Router# show tcp nsr detail client all location 0/1/CPU0

============================================================
CCB 0x482bf378, Proc Name mpls_ldp
Instance ID 1, Job ID 360
Number of session-sets 1
Number of sessions 1
Number of NSR Synced sessions 1
Connected at: Sun Jun 10 07:05:41 2007
Registered for notifications: Yes

============================================================
CCB 0x482bd32c, Proc Name mpls_ldp
Instance ID 2, Job ID 361
Number of session-sets 1
Number of sessions 2
Number of NSR Synced sessions 2
Connected at: Sun Jun 10 07:06:01 2007
Registered for notifications: Yes
```

show tcp nsr detail endpoint

To display detailed information about the nonstop routing (NSR) end-points, use the **show tcp nsr detail endpoint** command in XR EXEC mode.

show tcp nsr detail endpoint [**location** { **all** | *node-id* }]

Syntax Description

end-point	Displays detailed info about the SSO/NSR local and partner endpoints.
location { **all** | *node-id* }	(Optional) Displays client information for the designated node or all the nodes.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Apart from Tusing this command to show local and partner node end-point information in details, you can also use this command can be used in debugging of TCP NSR issues.

Examples

The following sample output shows detailed information for all end-points:

```
Router# show tcp nsr detail endpoint

--------------------------------------------------------------
                     Node: 0/RP0/CPU0
--------------------------------------------------------------

Local endpoint:
  Node id: 0x2000
  Endp handl: 0x7f6f7400c6a8

  Endp len: 46
  Bytestream:
0xaf2f6465762f69702f7463705f73736f10804018b2080c8e4c0b3aa8daa80128abcb130b5f9138ac81808
  Service name: /dev/ip/tcp_sso/8192
```

show tcp nsr detail pcb

To display detailed information about the nonstop routing (NSR) state of TCP connections, use the **show tcp nsr detail pcb** command in XR EXEC mode.

show tcp nsr detail pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	PCB address range for the specific connection information. 0 to ffffffff. For example, the address range can be 0x482c6b8c.
all	Specifies all the connections.
location *node-id*	(Optional) Displays connection information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows the complete details for NSR for all locations:

```
RP/0/RP0/CPU0:router# show tcp nsr detail pcb all location 0/0/cpu0


==============================================================
PCB 0x482b6b0c, Client PID: 2810078
Local host: 5.1.1.1, Local port: 646
Foreign host: 5.1.1.2, Foreign port: 31466
SSCB 0x482bc80c, Client PID 2810078
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x00001000

NSR State: Up, Rcv Path Replication only: No
Replicated to standby: Yes
Synchronized with standby: Yes
FSSN: 3005097735, FSSN Offset: 0

Sequence number of last or current initial sync: 1181461961
Initial sync started at: Sun Jun 10 07:52:41 2007
Initial sync ended   at: Sun Jun 10 07:52:41 2007

Number of incoming packets currently held: 1
```

```
          Pak#    SeqNum     Len     AckNum
         -----  ----------  -----  ----------
             1  3005097735      0  1172387202

Number of iACKS currently held: 0

==============================================================
PCB 0x482c2920, Client PID: 2810078
Local host: 5.1.1.1, Local port: 646
Foreign host: 5.1.1.2, Foreign port: 11229
SSCB 0x482bb3bc, Client PID 2810078
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x00001000

NSR State: Down, Rcv Path Replication only: No
Replicated to standby: No
Synchronized with standby: No
NSR-Down Reason: Initial sync was aborted
NSR went down at: Sun Jun 10 11:55:38 2007

Initial sync in progress: No
Sequence number of last or current initial sync: 1181476338
Initial sync error, if any: 'ip-tcp' detected the 'warning' condition 'Initial sync operation
 timed out'
Source of initial sync error: Local TCP
Initial sync started at: Sun Jun 10 11:52:18 2007
Initial sync ended   at: Sun Jun 10 11:55:38 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

==============================================================
PCB 0x482baea0, Client PID: 2810078
Local host: 5.1.1.1, Local port: 646
Foreign host: 5.1.1.2, Foreign port: 41149
SSCB 0x482bb3bc, Client PID 2810078
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x00001000

NSR State: Down, Rcv Path Replication only: No
Replicated to standby: No
Synchronized with standby: No
NSR-Down Reason: Initial sync was aborted
NSR went down at: Sun Jun 10 11:55:38 2007

Initial sync in progress: No
Sequence number of last or current initial sync: 1181476338
Initial sync error, if any: 'ip-tcp' detected the 'warning' condition 'Initial sync operation
 timed out'
Source of initial sync error: Local TCP
Initial sync started at: Sun Jun 10 11:52:18 2007
Initial sync ended   at: Sun Jun 10 11:55:38 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

==============================================================
PCB 0x482c35ac, Client PID: 2859233
Local host: 5:1::1, Local port: 8889
Foreign host: 5:1::2, Foreign port: 14008
SSCB 0x4827fea8, Client PID 2859233
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x0000001c

NSR State: Up, Rcv Path Replication only: No
```

```
Replicated to standby: Yes
Synchronized with standby: Yes
FSSN: 2962722865, FSSN Offset: 0

Sequence number of last or current initial sync: 1181474373
Initial sync started at: Sun Jun 10 11:19:33 2007
Initial sync ended   at: Sun Jun 10 11:19:33 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

==============================================================
PCB 0x482c2f10, Client PID: 2859233
Local host: 5:1::1, Local port: 8889
Foreign host: 5:1::2, Foreign port: 40522
SSCB 0x4827fea8, Client PID 2859233
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x0000001b

NSR State: Up, Rcv Path Replication only: No
Replicated to standby: Yes
Synchronized with standby: Yes
FSSN: 3477316401, FSSN Offset: 0

Sequence number of last or current initial sync: 1181474373
Initial sync started at: Sun Jun 10 11:19:33 2007
Initial sync ended   at: Sun Jun 10 11:19:33 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0
```

show tcp nsr detail session-set

To display the detailed information about the nonstop routing (NSR) state of the session sets on different nodes, use the **show tcp nsr detail session-set** command in XR EXEC mode.

show tcp nsr detail session-set {*sscb-address* | **all**} [**location** *node-id*]

Syntax Description

sscb-address	Session-Set Control Block (SSCB) address range for the specific session set information. 0 to ffffffff. For example, the address range can be 0x482c6b8c.
all	Specifies all the session sets.
location *node-id*	(Optional) Displays information for session sets for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows all the session sets:

```
RP/0/RP0/CPU0:router# show tcp nsr detail session-set all


==============================================================
SSCB 0x482bc80c, Client PID: 2810078
Set Id: 1, Addr Family: IPv4
Role: Active, Protected by: 0/1/CPU0, Well known port: 646
Sessions: total 1, synchronized 1
Initial sync in progress: No
        Sequence number of last or current initial sync: 1181461961
        Number of sessions in the initial sync: 1
        Number of sessions already synced: 1
        Number of sessions that failed to sync: 0
        Initial sync started at: Sun Jun 10 07:52:41 2007
        Initial sync ended   at: Sun Jun 10 07:52:41 2007

==============================================================
SSCB 0x482bb3bc, Client PID: 2810078
Set Id: 2, Addr Family: IPv4
Role: Active, Protected by: 0/1/CPU0, Well known port: 646
```

```
Sessions: total 2, synchronized 0
Initial sync in progress: Yes
        Sequence number of last or current initial sync: 1181476338
        Initial sync timer expires in 438517602 msec
        Number of sessions in the initial sync: 2
        Number of sessions already synced: 0
        Number of sessions that failed to sync: 0
        Initial sync started at: Sun Jun 10 11:52:18 2007

==============================================================
SSCB 0x4827fea8, Client PID: 2859233
Set Id: 1, Addr Family: IPv6
Role: Active, Protected by: 0/1/CPU0, Well known port: 8889
Sessions: total 2, synchronized 2
Initial sync in progress: No
        Sequence number of last or current initial sync: 1181474373
        Number of sessions in the initial sync: 2
        Number of sessions already synced: 2
        Number of sessions that failed to sync: 0
        Initial sync started at: Sun Jun 10 11:19:33 2007
        Initial sync ended   at: Sun Jun 10 11:19:33 2007
```

show tcp nsr session-set brief

To display brief information about the session sets for the nonstop routing (NSR) state on different nodes, use the **show tcp nsr session-set brief** command in XR EXEC mode.

show tcp nsr session-set brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for session sets for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

A session set consists of a subset of the application’s session in which the subset is protected by only one standby node. The TCP NSR state machine operates with respect to these session sets.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows all the session sets that are known to the TCP instance:

```
RP/0/RP0/CPU0:router# show tcp nsr session-set brief

--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------
SSCB               Client    LocalAPP    Set-Id Family  State  Protect-Node Total/US/DS
0x00007f9e14022508  4776    mpls_ldp#1     646   IPv4   SAYN   0/RP1/CPU0   5/0/5
0x00007f9e14022778  4776    mpls_ldp#1     647   IPv6   SAYN   0/RP1/CPU0   0/0/0
0x00007f9e14025018  5714         bgp#1       1   IPv4   SAYN   0/RP1/CPU0  58/0/58
0x00007f9e140257a8  5714         bgp#1       2   IPv6   SAYN   0/RP1/CPU0   2/0/2
```

The following sample output shows brief information about the session sets for location 0/RP0/CPU0:

```
RP/0/RP0/CPU0:router# show tcp nsr session-set brief location 0/RP0/CPU0

--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------
SSCB               Client    LocalAPP    Set-Id Family  State  Protect-Node Total/US/DS
0x00007f9e14022508  4776    mpls_ldp#1     646   IPv4   SAYN   0/RP1/CPU0   5/0/5
0x00007f9e14022778  4776    mpls_ldp#1     647   IPv6   SAYN   0/RP1/CPU0   0/0/0
```

```
0x00007f9e14025018  5714         bgp#1       1   IPv4   SAYN   0/RP1/CPU0  58/0/58
0x00007f9e140257a8  5714         bgp#1       2   IPv6   SAYN   0/RP1/CPU0   2/0/2
```

This table describes the significant fields shown in the display.

Table 73: show tcp nsr session-set brief Command Field Descriptions

Field	Description
SSCB	Unique ID for Session-Set Control Block (SSCB) to identify a session-set of a client.
Client	PID of the client process.
LocalAPP	Name and instance number of the client process.
Set-Id	ID of the session-set.
Family	Address family of the sessions added to the session set for IPv4 or IPv6.
Role	Role of the TCP stack for active or standby.
Protect-Node	Node that is offering the protection, for example, partner node.
Total/Synced	Total number of sessions in the set versus the sessions that have been synchronized.

show tcp nsr statistics client

To display the nonstop routing (NSR) statistics for the clients, use the **show tcp nsr statistics client** command in XR EXEC mode.

show tcp nsr statistics client {*ccb-address* | **all**} [**location** *node-id*]

Syntax Description

ccb-address	Client Control Block (CCB) address range for the specific statistics information for the client. 0 to ffffffff. For example, the address range can be 0x482c6b8c.
all	Specifies all the statistics for the clients.
location *node-id*	(Optional) Displays statistics for the client for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows all the statistics for the client:

```
RP/0/RP0/CPU0:router# show tcp nsr statistics client all


============================================================
CCB: 0x482b25d8
Name: mpls_ldp, Job ID: 360
Connected at: Thu Jan  1 00:00:00 1970

Notification Stats      : Queued  Failed  Delivered  Dropped
Init-Sync Done          :      0       0          0       0
Replicated Session Ready:      0       0          0       0
Operational Down        :      0       0          0       0
Last clear at: Sun Jun 10 12:19:12 2007


============================================================
CCB: 0x4827fd30
Name: mpls_ldp, Job ID: 361
Connected at: Sun Jun 10 07:05:54 2007
```

```
Notification Stats      : Queued  Failed  Delivered  Dropped
Init-Sync Done          :      1       0          1       0
Replicated Session Ready:      0       0          0       0
Operational Down        :      0       0          0       0
Last clear at: Never Cleared
```

show tcp nsr statistics npl

To display the nonstop routing (NSR) summary statistics across all TCP sessions of NPL clients, use the **show tcp nsr statistics npl** command in XR EXEC mode.

show tcp nsr statistics npl [**location** { **all** | *node-id* }]

Syntax Description

location *node-id*	(Optional) Displays information for the summary statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Although this command gives information about packet sent, received, dropped at NSR NPL based on queue priority, it is mostly used for debugging.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows the summary statistics sacross all TCP sessions of NPL clients:

```
Router# show tcp nsr statistics npl location all

--------------------------------------------------------------
                     Node: 0/0/CPU0
--------------------------------------------------------------


Prio Queue: Low
----------------
        Msg-type                                          Number
        -------------------------------------------------------------
        Sent Data                   :                      74

        Recv Data                   :                       4


        ****Drop Stats****

        Msg-type              Drop-reason                     Number
        -------------------------------------------------------------
        Send Drop:      <None>
        Recv Drop:      <None>


Prio Queue: High
```

```
----------------
        Msg-type                                          Number
        -------------------------------------------------------------
        Sent Data                   :                      13
        Sent Ack                    :                       7

        Recv Data                   :                      11
        Recv Ack                    :                      11


        ****Drop Stats****

        Msg-type              Drop-reason                     Number
        -------------------------------------------------------------
        Send Drop:      <None>
        Recv Drop:      <None>

--------------------------------------------------------------
                     Node: 0/2/CPU0
--------------------------------------------------------------


Prio Queue: Low
----------------
        Msg-type                                          Number
        -------------------------------------------------------------
        Sent Data                   :                       4

        Recv Data                   :                      74


        ****Drop Stats****

        Msg-type              Drop-reason                     Number
        -------------------------------------------------------------
        Send Drop:      <None>
        Recv Drop:      <None>


Prio Queue: High
----------------
        Msg-type                                          Number
        -------------------------------------------------------------
        Sent Data                   :                      11
        Sent Ack                    :                      11

        Recv Data                   :                      13
        Recv Ack                    :                       7


        ****Drop Stats****

        Msg-type              Drop-reason                     Number
        -------------------------------------------------------------
        Send Drop:      <None>
        Recv Drop:      <None>
```

show tcp nsr statistics pcb

To display the nonstop routing (NSR) statistics for a given Protocol Control Block (PCB), use the **show tcp nsr statistics pcb** command in XR EXEC mode.

show tcp nsr statistics pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	PCB address range for the specific connection information. 0 to ffffffff. For example, the address range can be 0x482c6b8c.
all	Specifies all the connection statistics.
location *node-id*	(Optional) Displays connection statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows all NSR statistics:

```
RP/0/RP0/CPU0:router# show tcp nsr statistics pcb all

--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------

==============================================================
PCB 0x7f9e3c028538
Number of times NSR went up: 1
Number of times NSR went down: 0
Number of times NSR was disabled: 0
Number of times switch-over occured : 0
IACK RX Message Statistics:
Number of iACKs dropped because session is not replicated : 0
Number of iACKs dropped because init-sync is in 1st phase : 1
Number of stale iACKs dropped : 0
Number of iACKs not held because of an immediate match : 0
TX Messsage Statistics:
Data transfer messages:
Sent 47, Dropped 0, Data (Total/Avg.) 23021748224/489824430
```

```
IOVAllocs : 0
Rcvd 0
Success : 0
Dropped (Trim) : 0
Dropped (Buf. OOS): 0
Segmentation instructions:
Sent 105, Dropped 0, Units (Total/Avg.) 1862270976/17735914
Rcvd 0
Success : 0
Dropped (Trim) : 0
Dropped (TCP) : 0
NACK messages:
Sent 0, Dropped 0
Rcvd 0
Success : 0
Dropped (Data snd): 0
Cleanup instructions :
Sent 46, Dropped 0
Rcvd 0
Success : 0
Dropped (Trim) : 0
Last clear at: Never Cleared
```

show tcp nsr statistics session-set

To display the nonstop routing (NSR) statistics for a session set, use the **show tcp nsr statistics session-set** command in XR EXEC mode.

show tcp nsr statistics session-set {*sscb-address* | **all**} [**location** *node-id*]

Syntax Description

sscb-address	Session-Set Control Block (SSCB) address range for the specific session set information for the statistics. 0 to ffffffff. For example, the address range can be 0x482b3444.
all	Specifies all the session sets for the statistics.
location *node-id*	(Optional) Displays session set information for the statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows all session set information for the statistics:

```
RP/0/RP0/CPU0:router# show tcp nsr statistics session-set all

--------------------------------------------------------------
Node: 0/RP0/CPU0
--------------------------------------------------------------

===================Session Set Stats ===========================
SSCB 0x7f9e14022508, Set ID: 646
Number of times init-sync was attempted :0
Number of times init-sync was successful :0
Number of times init-sync failed :0
Number of times switch-over occured :0
Number of times NSR has been reset :0
Last clear at: Wed Dec 2 20:44:48 2015


===================Session Set Stats ===========================
SSCB 0x7f9e14022778, Set ID: 647
Number of times init-sync was attempted :0
Number of times init-sync was successful :0
Number of times init-sync failed :0
Number of times switch-over occured :0
Number of times NSR has been reset :0
Last clear at: Wed Dec 2 20:44:48 2015


===================Session Set Stats ===========================
SSCB 0x7f9e14025018, Set ID: 1
Number of times init-sync was attempted :0
Number of times init-sync was successful :0
Number of times init-sync failed :0
Number of times switch-over occured :0
Number of times NSR has been reset :0
Last clear at: Wed Dec 2 20:44:48 2015


===================Session Set Stats ===========================
SSCB 0x7f9e140257a8, Set ID: 2
Number of times init-sync was attempted :0
Number of times init-sync was successful :0
Number of times init-sync failed :0
Number of times switch-over occured :0
Number of times NSR has been reset :0
Last clear at: Wed Dec 2 20:44:48 2015
```

show tcp nsr statistics summary

To display the nonstop routing (NSR) summary statistics across all TCP sessions, use the **show tcp nsr statistics summary** command in XR EXEC mode.

show tcp nsr statistics summary [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the summary statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

If a value is not specified, the current RP in which the command is being executed is taken as the location.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The **location** keyword is used so that active and standby TCP instances are independently queried.

Task ID

Task ID	Operations
transport	read

Examples

The following sample output shows the summary statistics for all TCP sessions:

```
Router# show tcp nsr statistics summary

=====================Summary Stats========================
Last clear at: Never Cleared
Notif Statistics:
Queued Failed Delivered Dropped
Init-sync Done : 7 0 7 0
Replicated Session Ready: 0 0 0 0
Operational Down : 0 0 0 0
Init-sync Stop Reading : 7 0 7 0
Clients Statistics:
Number of Connected Clients :2
Number of Disconnected Clients :0
Number of Current Clients :2
Session Sets Statistics:
Number of Created Session Sets :4
Number of Destroyed Session Sets:0
Number of Current Session Sets :4
Sessions Statistics:
Number of Added Sessions :65
Number of Deleted Sessions :0
Number of Current Sessions :65
InitSync Statistics:
Number of times init-sync was attempted :7
Number of times init-sync was successful :7
Number of times init-sync failed :0
```

```
Held packets and iacks Statistics:
Number of packets held by Active TCP :67
Number of held packets dropped by Active TCP :0
Number of iacks held by Active TCP :0
Number of held iacks dropped by Active TCP :0
Number of iacks sent by Standby TCP :0
Number of iacks received by Active TCP :0
QAD Msg Statistics:
Number of dropped messages from partner TCP stack(s) : 0
Number of unknown messages from partner TCP stack(s) : 0
Number of messages accepted from partner TCP stack(s) : 1341
Number of stale dropped messages from partner TCP stack(s) : 0
Number of messages sent to partner TCP stack(s) : 22480
Number of messages failed to be sent to partner TCP stack(s): 0
RX Msg Statistics:
Number of iACKs dropped because there is no PCB : 0
Number of iACKs dropped because there is no datapath SCB : 0
Number of iACKs dropped because session is not replicated : 0
Number of iACKs dropped because init-sync is in 1st phase : 1056
Number of stale iACKs dropped : 17
Number of iACKs not held because of an immediate match : 0
Number of held packets dropped because of errors : 0
TX Messsage Statistics:
Data transfer messages:
Sent 4533, Dropped 0
IOVAllocs : 0
Rcvd 0
Success : 0
Dropped (PCB) : 0
Dropped (SCB-DP) : 0
Dropped (Trim) : 0
Dropped (Buf. OOS): 0
Segmentation instructions:
Sent 14124, Dropped 0
Rcvd 0
Success : 0
Dropped (PCB) : 0
Dropped (SCB-DP) : 0
Dropped (Trim) : 0
Dropped (TCP) : 0
NACK messages:
Sent 0, Dropped 0
Rcvd 0
Success : 0
Dropped (PCB) : 0
Dropped (SCB-DP) : 0
Dropped (Data snd): 0
Cleanup instructions :
Sent 3608, Dropped 0
Rcvd 0
Success : 0
Dropped (PCB) : 0
Dropped (SCB-DP) : 0
Dropped (Trim) : 0
Audit Messsage Statistics:
Mark Session set messages:
Sent 0, Dropped 0
Rcvd 0
Dropped : 0
Audit Session messages:
Sent 0, Dropped 0
Rcvd 0
Dropped : 0
Sweep Session set messages:
```

```
Sent 0, Dropped 0
Rcvd 0
Dropped : 0
Session set audit response messages:
Sent 0, Dropped 0
Rcvd 0
Dropped : 0
Mark Session set ack messages:
Sent 0, Dropped 0
Rcvd 0
Dropped : 0
Mark Session set nack messages:
Sent 0, Dropped 0
Rcvd 0
Dropped : 0
Number of audit operations aborted: 0
```

show tcp packet-trace

To display the details of the packet traces of a PCB, use the **show tcp packet-trace** command in XR EXEC mode.

show tcp packet-trace *pcb-name* **location** *node-id*

Syntax Description

pcb-name	Displays packet traces for the specified PCB.
location *node-id*	(Optional) Clears the TCP connection for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Apart from using this command to provide packet trace of a particular TCP PCB, you can also use this command for debugging purposes or to monitor flow of TCP packets for a TCP connection if you configure the pak-rate for the TCP PCB.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp packet-trace 0x00007f7d4c035378**command:

```
Router# show tcp packet-trace 0x00007f7d4c035378

==============================================================
Packet traces for: PCB 0x7f7d4c035378, 133.1.2.2:25032 <-> 133.1.2.1:179, VRF 0x60000000

May 14 05:50:59.463>R --A--- SEQ 2125620474 ACK 3607271508 LEN     0 WIN 31533 (pak:
0x63bfeedb, line: 3855)
                    snduna 3607271489 sndnxt 3607271508 sndmax 3607271508 sndwnd 31552
                    rcvnxt 2125620474 rcvadv 2125653242 rcvwnd 32768
                    ao_option 0
May 14 05:50:59.463>D --A--- SEQ 2125620474 ACK 3607271508 LEN     0 WIN 31533 (pak:
0x63bfeedb, line: 932)
                    snduna 3607271508 sndnxt 3607271508 sndmax 3607271508 sndwnd 31533
                    rcvnxt 2125620474 rcvadv 2125653242 rcvwnd 32768
                    ao_option 0
May 14 05:51:15.719>R --A--- SEQ 2125620474 ACK 3607271508 LEN  1460 WIN 31533 (pak:
0x63bfeedb, line: 3855)
                    snduna 3607271508 sndnxt 3607271508 sndmax 3607271508 sndwnd 31533
                    rcvnxt 2125620474 rcvadv 2125653242 rcvwnd 32768
.
.
```

```
.
.
.
May 14 05:57:45.953>R --A-P- SEQ 2125717138 ACK 3607271622 LEN   496 WIN 31419 (pak:
0x63bffcbb, line: 3855)
                    snduna 3607271622 sndnxt 3607271622 sndmax 3607271622 sndwnd 31419
                    rcvnxt 2125717138 rcvadv 2125748446 rcvwnd 31308
                    ao_option 0
May 14 05:57:45.953>S --A--- SEQ 3607271622 ACK 2125717634 LEN     0 WIN   128 (pak:
0x63bffcbb, line: 2688)
                    snduna 3607271622 sndnxt 3607271622 sndmax 3607271622 sndwnd 31419
                    rcvnxt 2125717634 rcvadv 2125750402 rcvwnd 32768
                    ao_option 0
May 14 05:57:45.953>R (app read)
                    snduna 3607271622 sndnxt 3607271622 sndmax 3607271622 sndwnd 31419
                    rcvnxt 2125717634 rcvadv 2125750402 rcvwnd 32768
                    ao_option 0
```

show tcp pak-rate

To display the details of the packet rate of a PCB, for example, number of packets received, maximum packet-size in the last 30 seconds, number of packets allocated, and number of packets freed, use the **show tcp pak-rate** command in XR EXEC mode if 'pak-rate tcp stats-start is configured.

show tcp pak-rate { **mem-summary** | | **stats** } { **location** *node-id* }

Syntax Description

mem-summary	Displays the memory summary of the TCP packet rate of a PCB.
stats	Displays the statistics of the TCP packet rate of a PCB.
location *node-id*	(Optional) Clears the TCP connection for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp pak-rate mem-summary location 0/RP0/CPU0**command:

```
Router# show tcp pak-rate mem-summary location 0/0/CPU0


 Family  Index  Num Allocs  Num frees
 -----------------------------------
  IPv4     0          0          0
  IPv4     1          0          0
  IPv4     2          0          0
  IPv4     3          0          0
  IPv4     4          0          0
  IPv4     5          0          0
  IPv4     6          0          0
  IPv4     7          0          0
  IPv4     8          0          0
  IPv4     9          0          0
  IPv6     0          0          0
  IPv6     1          0          0
  IPv6     2          0          0
  IPv6     3          0          0
  IPv6     4          0          0
  IPv6     5          0          0
```

```
IPv6     6           0           0
IPv6     7           0           0
IPv6     8           0           0
IPv6     9           0           0
```

show tcp statistics

To display TCP statistics, use the **show tcp statistics** command in XR EXEC mode.

show tcp statistics {**client** | **pcb** {**all** *pcb-address*} | **summary** } [**location** *node-id*]

Syntax Description

client	Displays statistics of TCP clients.
pcb *pcb-address*	(Optional) Displays detailed statistics for a specified connection.
pcb all	(Optional) Displays detailed statistics for all connections.
summary	(Optional) Clears summary statistic for a specific node or connection.
location *node-id*	(Optional) Displays statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp statistics** command:

```
RP/0/RP0/CPU0:router# show tcp statistics pcb 0x08091bc8

Statistics for PCB 0x8091bc8 VRF Id 0x60000000
Send:    0 bytes received from application
         0 xipc pulse received from application
         0 bytes sent to network
         0 packets failed getting queued to network
Rcvd:    0 packets received from network
         0 packets queued to application
         0 packets failed queued to application
```

This table describes the significant fields shown in the display.

Table 74: show tcp statistics Command Field Descriptions

Field	Description
vrfid	VPN routing and forwarding (VRF) identification (vrfid) number.
Send	Statistics in this section refer to packets sent by the router.
Rcvd:	Statistics in this section refer to packets received by the router.

show udp brief

To display a summary of the User Datagram Protocol (UDP) connection table, use the **show udp brief** command in XR EXEC mode.

show udp brief [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp brief** command:

```
RP/0/RP0/CPU0:router# show udp brief



PCB        VRF-ID Recv-Q Send-Q Local Address Foreign Address
0x7fb44c029678 0x60000000 0       0 :::35333       :::0
0x7fb44c028fa8 0x00000000 0       0 :::35333       :::0
0x7fb43000b708 0x60000000 0       0 :::49270       :::0
0x7fb43000b038 0x00000000 0       0 :::49270       :::0
0x7fb43001fbb8 0x60000000 0       0 :::123         :::0
0x7fb430010f28 0x00000000 0       0 :::123         :::0
0x7fb430009ea8 0x60000000 0       0 :::41092       :::0
0x7fb4300096b8 0x00000000 0       0 :::41092       :::0
0x7fb44c025008 0x60000000 0       0 :::161         :::0
0x7fb43000cda8 0x60000001 0       0 :::161         :::0
0x7fb43000d2d8 0x60000002 0       0 :::161         :::0
0x7fb43000d938 0x60000003 0       0 :::161         :::0
0x7fb43000df98 0x60000004 0       0 :::161         :::0
0x7fb43000e5f8 0x60000005 0       0 :::161         :::0
0x7fb43000ec58 0x60000006 0       0 :::161         :::0
0x7fb43000f2b8 0x60000007 0       0 :::161         :::0
0x7fb43000f918 0x60000008 0       0 :::161         :::0
0x7fb43000ff78 0x60000009 0       0 :::161         :::0
0x7fb4300046c8 0x00000000 0       0 :::161         :::0
0x7fb44c025f78 0x60000000 0       0 :::162         :::0
0x7fb44c02b1f8 0x60000001 0       0 :::162         :::0
```

```
0x7fb44c02b848 0x60000002 0       0 :::162         :::0
0x7fb44c02bea8 0x60000003 0       0 :::162         :::0
0x7fb44c02c508 0x60000004 0       0 :::162         :::0
0x7fb44c02cb68 0x60000005 0       0 :::162         :::0
0x7fb44c02d1c8 0x60000006 0       0 :::162         :::0
0x7fb44c02d828 0x60000007 0       0 :::162         :::0
0x7fb44c02de88 0x60000008 0       0 :::162         :::0
0x7fb44c02e4e8 0x60000009 0       0 :::162         :::0
0x7fb44c0258e8 0x00000000 0       0 :::162         :::0
0x7fb4300024d8 0x60000000 0       0 :::3503        :::0
0x7fb44c028628 0x60000000 0       0 :::32958       :::0
0x7fb44c028018 0x00000000 0       0 :::32958       :::0
0x7fb44c02a9e8 0x60000000 0       0 :::3799        :::0
0x7fb44c02a258 0x00000000 0       0 :::3799        :::0
0x7fb4300012e8 0x00000000 0       0 :::0           :::0
0x7fb44c023258 0x60000000 0       0 0.0.0.0:514   0.0.0.0:0
0x7fb44c027848 0x60000000 0       0 0.0.0.0:27202 0.0.0.0:0
0x7fb4300077e8 0x00000000 0       0 0.0.0.0:27202 0.0.0.0:0
0x7fb44c03cf48 0x60000000 0       0 0.0.0.0:123   0.0.0.0:0
0x7fb4300107e8 0x00000000 0       0 0.0.0.0:123   0.0.0.0:0
0x7fb430000c18 0x60000000 0       0 0.0.0.0:646   0.0.0.0:0
0x7fb44c022158 0x00000000 0       0 0.0.0.0:646   0.0.0.0:0
0x7fb44c0274e8 0x60000000 0       0 0.0.0.0:30613 0.0.0.0:0
0x7fb430006bf8 0x00000000 0       0 0.0.0.0:30613 0.0.0.0:0
0x7fb44c0270f8 0x60000000 0       0 0.0.0.0:50589 0.0.0.0:0
0x7fb430006008 0x00000000 0       0 0.0.0.0:50589 0.0.0.0:0
```

This table describes the significant fields shown in the display.

Table 75: show udp brief Command Field Descriptions

Field	Description
PCB	Protocol control block address. This is the address to a structure that contains connection information such as local address, foreign address, local port, foreign port, and so on.
Recv-Q	Number of bytes in the receive queue.
Send-Q	Number of bytes in the send queue.
Local Address	Local address and local port.
Foreign Address	Foreign address and foreign port.

show udp detail pcb

To display detailed information of the User Datagram Protocol (UDP) connection table, use the **show udp detail pcb** command in XR EXEC mode.

show udp detail pcb {*pcb-address* | **all**} [**location** *node-id*]

Syntax Description

pcb-address	Address of a specified UDP connection.
all	Provides statistics for all UDP connections.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp detail pcb all** command:

```
RP/0/RP0/CPU0:router# show udp detail pcb all location 0/RP0/CPU0

===============================================
PCB is 0x4822fea0, Family: 2, VRF: 0x60000000
 Local host: 0.0.0.0:3784
 Foreign host: 0.0.0.0:0

Current send queue size: 0
Current receive queue size: 0
===============================================
PCB is 0x4822d0e0, Family: 2, VRF: 0x60000000
 Local host: 0.0.0.0:3785
 Foreign host: 0.0.0.0:0

Current send queue size: 0
Current receive queue size: 0
```

This table describes the significant fields shown in the display.

Table 76: show raw pcb Command Field Descriptions

Field	Description
PCB	Protocol control block address.
Family	Network protocol. IPv4 is 2; IPv6 is 26.
VRF	VPN routing and forwarding (VRF) instance name.
Local host	Local host address.
Foreign host	Foreign host address.
Current send queue size	Size of the send queue (in bytes).
Current receive queue size	Size of the receive queue (in bytes).

show udp extended-filters

To display the details of the UDP extended-filters, use the **show udp extended-filters** command in XR EXEC mode.

show udp extended-filters {**location** *node-id* | **peer-filter** {**location** *node-id*}}

Syntax Description

location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
peer-filter	Displays connections with peer filter configured.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp extended-filters** command for a specific location (0/RP0/CPU0):

```
RP/0/RP0/CPU0:router# show udp extended-filters location 0/RP0/CPU0


JID: 1111
Family: 10
VRF: 0x60000000
PCB: 0x7fb44c029678
L4-proto: 17
Lport: 35333
Fport: 0
Laddr: 70:8653:f7f:0:303d:40ba:3200:0
Faddr: e297:ba:3200:0:3208::
ICMP error filter mask: 0x0
LPTS options: 0x0 / 0x5 / 0x0 / BOUND /
Flow Type: RADIUS
```

show udp statistics

To display User Datagram Protocol (UDP) statistics, use the **show udp statistics** command in XR EXEC mode.

show udp statistics { **clients** | **pcb** { **all** | *pcb-address* } | **summary** } [**location** *node-id*]

Syntax Description

clients	(Optional) Clears statistics for all TCP clients.
pcb *pcb-address*	Displays detailed statistics for each connection.
pcb *all*	Displays detailed statistics for all connections.
location *node-id*	(Optional) Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	Displays summary statistics.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

UDP clones the received packets if there are multiple multicast applications that are interested in receiving those packets.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp statistics summary** command:

```
Router# show udp statistics summary

UDP statistics:
Rcvd: 121 Total, 121 drop, 0 no port
      0 checksum error, 0 too short
Sent: 121 Total, 0 error
0 Total forwarding broadcast packets
0 Cloned packets, 0 failed cloning
```

This table describes the significant fields shown in the display.

Table 77: show udp Command Field Descriptions

Field	Description
Rcvd: Total	Total number of packets received.
Rcvd: drop	Total number of packets received that were dropped.
Rcvd: no port	Total number of packets received that have no port.
Rcvd: checksum error	Total number of packets received that have a checksum error.
Rcvd: too short	Total number of packets received that are too short for UDP packets.
Sent: Total	Total number of packets sent successfully.
Sent: error	Total number of packets that cannot be sent due to errors.
Total forwarding broadcast packets	Total number of packets forwarded to the helper address.
Cloned packets	Total number of packets cloned successfully.
failed cloning	Total number of packets that failed cloning.

tcp dump-file convert

To convert the TCP dump packet traces files to other readable formats such as pcap, text, or both, use **tcp dump-file convert** command in XR EXEC mode.

tcp dump-file convert { *pcap* | *text* | *all-formats* } { *all* | *binary_file_name* | *ipaddress* } **location** { *node-id* } **file** { *absolute file path* }

Syntax Description

pcap	Converts TCP dump packet traces files to pcap format.
text	Converts TCP dump packet traces files to text format.
all-format	Converts TCP dump packet traces files to both pcap and text format.
all	Collects TCP dump file data from all peers and nodes.
binary_file_name	Specifies the name of the dump file to be converted.
ipaddress	Specifies the IP address of the peer node.
location {*node-id*}	(Optional) Specifies the node to store the converted TCP dump file. The *node-id* is entered in the *rack/slot/module* notation, for example **location** *0/RP0/CPU0*. By default, the files are stored in the current node where the CLI command is executed.
file {*absolute file path* }	(Optional) Specifies the absolute file path where you want to store the converted TCP dump files. The file path is entertered in the *node/filename* notation, for example */harddisk:/demo1*. By default, the converted files are stored inside the file "decoded_dumpfiles" in the current node where the CLI command is executed or if you have provided the location the files are stored in that location.

Command Default

No default behavior or values.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 24.2.11	This command was introduced.

Usage Guidelines

Use this command to convert TCP dump packet traces files into text, pcap, or both readable formats.

Examples

The following example shows how to convert TCP packet traces files into text and pcap readable formats:

```
Router# tcp dump-file convert all-formats all
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_53.462070.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_10_8_40.154838.pcap
[OK]
```

The following example shows how to filter TCP dump packet traces by ip address and convert them into text and pcap readable format:

```
Router# tcp dump-file convert all-formats ipaddress 1.1.1.2
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_1_1_1_2_node0_RSP0_CPU0_2024_3_19_10_9_20.539021.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_1_1_1_2_node0_RSP0_CPU0_2024_3_19_10_9_20.539021.pcap
[OK]
```

The following example specifies a location where you want to store the converted TCP dump file:

```
Router# tcp dump-file convert all-formats all location 0/RP0/CPU0
ascii file is saved at :
/harddisk:/decoded_dumpfiles/text_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_12_53_35.12323.txt
pcap file is saved at :
/harddisk:/decoded_dumpfiles/pcap_tcpdump_peer_all_node0_RP0_CPU0_2024_3_19_12_53_35.12323.pcap
[OK]
```

The following example specifies the absolute file path where you want to store the converted TCP dump files:

```
Router# tcp dump-file convert text all file /harddisk:/demo2
ascii file is saved at : /harddisk:/demo2.txt
[OK]
```

tcp mss

To configure the TCP maximum segment size that determines the size of the packet that TCP uses for sending data, use the **tcp mss** command in XR Config mode.

tcp mss *segment-size*

Syntax Description

segment-size	Size, in bytes, of the packet that TCP uses to send data. Range is 68 to 10000 bytes.

Command Default

If this configuration does not exist, TCP determines the maximum segment size based on the settings specified by the application process, interface maximum transfer unit (MTU), or MTU received from Path MTU Discovery.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read, write

Examples

This example shows how to configure the TCP maximum segment size:

```
RP/0/RSP0/CPU0:router(config)# tcp mss 1460
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them? [yes]:
RP/0/RSP0/CPU0:router:Sep  8 18:29:51.084 : config[65700]: %LIBTARCFG-6-COMMIT :

Configuration committed by user 'lab'.   Use 'show commit changes 1000000596' to view the
changes.
Sep  8 18:29:51.209 : config[65700]: %SYS-5-CONFIG_I : Configured from console by lab
```

tcp path-mtu-discovery

To allow TCP to automatically detect the highest common maximum transfer unit (MTU) for a connection, use the **tcp path-mtu-discovery** in XR Config mode. To reset the default, use the **no** form of this command.

tcp path-mtu-discovery [**age-timer** *minutes* | **infinite**]
no tcp path-mtu-discovery

Syntax Description

age-timer *minutes*	(Optional) Specifies a value in minutes. Range is 10 to 30.
infinite	(Optional) Turns off the age timer.

Command Default

tcp path-mtu-discovery is disabled

age-timer default is 10 minutes

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **tcp path-mtu-discovery** command to allow TCP to automatically detect the highest common MTU for a connection, such that when a packet traverses between the originating host and the destination host the packet is not fragmented and then reassembled.

The age timer value is in minutes, with a default value of 10 minutes. The age timer is used by TCP to automatically detect if there is an increase in MTU for a particular connection. If the **infinite** keyword is specified, the age timer is turned off.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to set the age timer to 20 minutes:

```
RP/0/RP0/CPU0:router(config)# tcp path-mtu-discovery age-timer 20
```

tcp selective-ack

To enable TCP selective acknowledgment (ACK) and identify which segments in a TCP packet have been received by the remote TCP, use the **tcp selective-ack** command in XR Config mode. To reset the default, use the **no** form of this command.

tcp selective-ack
no tcp selective-ack

Syntax Description

XR Config mode

This command has no keywords or arguments.

Command Default

TCP selective ACK is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was supported.

Usage Guidelines

If TCP Selective ACK is enabled, each packet contains information about which segments have been received by the remote TCP. The sender can then resend only those segments that are lost. If selective ACK is disabled, the sender receives no information about missing segments and automatically sends the first packet that is not acknowledged and then waits for the other TCP to respond with what is missing from the data stream. This method is inefficient in Long Fat Networks (LFN), such as high-speed satellite links in which the bandwidth * delay product is large and valuable bandwidth is wasted waiting for retransmission.

Task ID

Task ID	Operations
transport	read, write

Examples

In the following example, the selective ACK is enabled:

```
RP/0/RP0/CPU0:router(config)# tcp selective-ack
```

tcp synwait-time

To set a period of time the software waits while attempting to establish a TCP connection before it times out, use the **tcp synwait-time** command in XR Config mode. To restore the default time, use the **no** form of this command.

tcp synwait-time *seconds*
no tcp synwait-time *seconds*

Syntax Description

seconds	Time (in seconds) the software waits while attempting to establish a TCP connection. Range is 5 to 30 seconds.

Command Default

The default value for the synwait-time is 30 seconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was supported.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to configure the software to continue attempting to establish a TCP connection for 18 seconds:

```
RP/0/RP0/CPU0:router(config)# tcp synwait-time 18
```

tcp timestamp

To more accurately measure the round-trip time of a packet, use the **tcp timestamp** command in XR Config mode. To reset the default, use the **no** form of this command.

tcp timestamp
no tcp timestamp

Syntax Description

This command has no keywords or arguments.

Command Default

A TCP time stamp is not used.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was supported.

Usage Guidelines

Use the **tcp timestamp** command to more accurately measure the round-trip time of a packet. If a time stamp is not used, a TCP sender deduces the round-trip time when an acknowledgment of its packet is received, which is not a very accurate method because the acknowledgment can be delayed, duplicated, or lost. If a time stamp is used, each packet contains a time stamp to identify packets when acknowledgments are received and the round-trip time of that packet.

This feature is most useful in Long Fat Network (LFN) where the bandwidth * delay product is long.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to enable the timestamp option:

```
RP/0/RP0/CPU0:router(config)# tcp timestamp
```

tcp window-size

To alter the TCP window size, use the **tcp window-size** command in XR Config mode. To restore the default value, use the **no** form of this command.

tcp window-size *bytes*
no tcp window-size

Syntax Description

bytes	Window size in bytes. Range is 2048 to 65535 bytes.

Command Default

The default value for the window size is 16k.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was supported.

Usage Guidelines

Do not use this command unless you clearly understand why you want to change the default value.

Task ID

Task ID	Operations
transport	read, write

Examples

The following example shows how to set the TCP window size to 3000 bytes:

```
RP/0/RP0/CPU0:router(config)# tcp window-size 3000
```

VRRP Commands

This chapter describes the commands used to configure and monitor Virtual Router Redundancy Protocol (VRRP) features.

For detailed information about VRRP concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco 8000 Series Routers*.

clear vrrp statistics

To reset the Virtual Router Redundancy Protocol (VRRP) statistics (to zero or default value), use the **clear vrrp statistics** command in XR EXEC mode.

clear vrrp statistics [**ipv4** | **ipv6**] [**interface type** *interface-path-id* | *vrid*]

Syntax Description

ipv4	(Optional) Resets the IPv4 VRRP statistics.
ipv6	(Optional) Resets the IPv6 VRRP statistics.
interface type	(Optional) Specifies the Interface type.
interface-path-id	(Optional) Specify a physical interface instance or a virtual interface instance for which VRRP statistics is cleared.
vrid	(Optional) Specify the virtual router identifier, which is the number identifying the virtual router for which VRRP statistics is cleared.

Command Default

No default behavior or values

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

If no interface is specified, the statistics for all virtual routers on all interfaces are cleared.

If no value for vrid is specified, the statistics for all virtual routers on the specified interface are cleared.

Task ID

Task ID	Operations
ip-services	execute

Examples

The following example shows how to clear vrrp statistics:

```
RP/0/RP0/CPU0:router# clear vrrp statistics
```

show vrrp

To display a brief or detailed status of one or all Virtual Router Redundancy Protocol (VRRP) virtual routers, use the **show vrrp** command in XR EXEC mode.

show **vrrp** [**ipv4** | **ipv6**] [**interface** *type* *interface-path-id*] [**brief** | **detail** | **statistics** [**all**]]

Syntax Description

ipv4	(Optional) Displays the IPv4 information.
ipv6	(Optional) Displays the IPv6 information.
interface	(Optional) Displays the status of the virtual router interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Provides a summary view of the virtual router information.
detail	(Optional) Displays detailed running state information.
statistics	(Optional) Displays total statistics.
all	(Optional) Displays statistics for each virtual router.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Release	Modification
Release 7.11.1	This command was modified. The fields **Mcast packet in Ucast mode**, **IPv4 Unicast Peer**, and **IPv4 Unicast Peer** were added.

Usage Guidelines

If no interface is specified, all virtual routers on all interfaces are displayed. If no vrid is specified, all vrids on the given interface are displayed.

Task ID

Task ID	Operations
vrrp	read

Examples

The following sample output is from the **show vrrp** command:

```
Router# show vrrp

                      A indicates IP address owner
                      | P indicates configured to preempt
                      | |
Interface   vrID Prio A P State    Master addr     VRouter addr
Te0/3/0/0      1  100   P Init     unknown         192.168.18.10
Te0/3/0/2      7  100   P Init     unknown         192.168.19.1
```

This table describes the significant fields shown in the display.

Table 78: show vrrp Command Field Descriptions

Field	Description
Interface	Interface of the virtual router.
vrID	ID of the virtual router.
Prio	Priority of the virtual router.
A	Indicates whether the VRRP router is the IP address owner.
P	Indicates whether the VRRP router is configured to preempt (default).
State	State of the virtual router.
Master addr	IP address of the IP address owner router.
VRouter addr	Virtual router IP address of the virtual router.

The following sample output is from the **show vrrp** command with the **detail** keyword:

```
Router# show vrrp detail
Fri Sep  8 15:02:35.268 IST
GigabitEthernet0/0/0/0 - IPv4 vrID 1
  State is Master
```

```
    2 state changes, last state change 04:00:02
    State change history:
    Sep  8 11:02:29.518 IST  Init     -> Backup   Virtual IP configured
    Sep  8 11:02:33.127 IST  Backup   -> Master   Master down timer expired
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is 10.0.0.100
  Virtual MAC address is 0000.5E00.0101, state is active
  Master router is local
  Version is 2
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
  IPv4 Unicast Peer: 10.0.1.1 --> IPv4 unicast transport is enabled on VRRP.

GigabitEthernet0/0/0/0 - IPv6 vrID 2
  State is Init
    0 state changes, last state change never
    State change history:
  Last resign sent:     Never
  Last resign received: Never
  Virtual IP address is ::
  Virtual MAC address is 0000.5E00.0202, state is stored
  Master router is unknown
  Version is 3
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + (156 x 1/256))
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
  IPv6 Unicast Peer: FE80::260:3EFF:FE11:6770 --> IPv6 unicast transport is enabled on VRRP.
```

This table describes the significant fields shown in the displays.

Table 79: show vrrp detail Command Field Descriptions

Field	Description
0/3/0/0 - vrID 1	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (IP address owner router or backup router).
Virtual IP address is	Virtual IP address for this virtual router.
Virtual MAC address is	Virtual MAC address for this virtual router.
Master router is	Location of the IP address owner router.
Advertise time	Interval (in seconds) at which the router sends VRRP advertisements when it is the IP address owner virtual router. This value is configured with the **vrrp timer** command.

Field	Description
Master Down Timer	Time the backup router waits for the IP address owner router advertisements before assuming the role of IP address owner router.
Minimum delay	Time that the state machine start-up is delayed when an interface comes up, giving the network time to settle. The minimum delay is the delay that is applied after any subsequent interface up event (if the interface flaps) and the reload delay is the delay applied after the first interface up event.
Current priority	Priority of the virtual router.
Configured priority	Priority configured on the virtual router.
may preempt	Indication of whether preemption is enabled or disabled.
minimum delay	Delay time before preemption (default) occurs.
Tracked items	Section indicating the items being tracked by the VRRP router.
Interface	Interface being tracked.
State	State of the tracked interface.
Priority Decrement	Priority to decrement from the VRRP priority when the interface is down.
IPv4 Unicast Peer	IPv4 address of the unicast peer.
IPv6 Unicast Peer	IPv6 address of the unicast peer.

The following sample output is from the **show vrrp** command with the **statistics** .

```
show vrrp statistics
Fri Sep  8 15:03:03.521 IST
Invalid packets:
  Invalid checksum:                    0
  Unknown/unsupported versions:        0
  Invalid vrID:                        0
  Too short:                           0
Protocol:
  Transitions to Master                1
Packets:
  Total received:                      0
  Adverts sent:                    14476
  Bad TTL:                             0
  Short Packets:                       0
  Failed authentication:               0
  Unknown authentication:              0
  Conflicting authentication:          0
  Unknown Type field:                  0
  Conflicting Advertise time:          0
  Conflicting Addresses:               0
  Received with zero priority:         0
  Sent with zero priority:             0
  Mcast packet in Ucast mode:          0
```

This table describes the significant fields shown in the displays.

Table 80: show vrrp statistics Command Field Descriptions

Field	Description
Invalid packets	Number of invalid packets.
Invalid checksum	Number of packets with checksum errors.
Unknown/unsupported versions	Number of packets with unknown/unsupported versions.
Invalid vrID	Number of packets with invalid VRRP ID
Too short	Number of packets that are too short.
Protocol	Role of the VRRP routers.
Transitions to Master	Number of VRRP routers that have taken over the master.
Packets	Number of packets received.
Total received	Cumulative number of packets received.
Adverts sent	Number of times the router has advertised its VRRP status.
Bad TTL	Number of packets with incorrect Time-to-Live values.
Short Packets	Number of packets with a size shorter than expected.
Failed authentication	Number of packets that failed authentication during VRRP operation.
Unknown authentication	Number of packets that failed authentication because the authentication was not recognized.
Conflicting authentication	Number of packets that failed authentication due to conflicts.
Conflicting IP addresses	Number of packets where conflicting IP addresses are detected within the VRRP configuration.
Received with zero priority	Number of packets received with zero priority.
Sent with zero priority	Number of packets sent by a VRRP router with a priority of zero.
Mcast packet in Ucast mode	Number of multicast packets received in a specific VRRP instance when it's configured to function in unicast mode.

The following sample output is from the **show vrrp** command with the **interface** for Ethernet interface 0/3/0/0:

```
Router# show vrrp interface Ethernet0/3/0/0

                      A indicates IP address owner
                      | P indicates configured to preempt
                      | |
Interface   vrID Prio A P State    Master addr     VRouter addr
```

```
Te0/3/0/0      1  100   P Init     unknown         192.168.10.20
Te0/3/0/2      7  100   P Init     unknown         192.168.20.0
```

show vrrp statistics

To display statistics of one or all Virtual Router Redundancy Protocol (VRRP) virtual routers, use the **show vrrp statistics** command in the XR EXEC mode.

show **vrrp** [**ipv4** | **ipv6**] [**interface type** *interface-path-id* | *vrid*] **statistics** [**all**]

Syntax Description

ipv4	(Optional) Displays the IPv4 information.
ipv6	(Optional) Displays the IPv6 information.
interface type	(Optional) Specifies the Interface type.
interface-path-id	(Optional) Specify a physical interface instance or a virtual interface instance.
vrid	(Optional) Specify the virtual router identifier, which is the number identifying the virtual router for which statistics is displayed.
all	(Optional) Displays statistics for each virtual router.

Command Default

No default behavior or values

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

If no interface is specified, the statistics for all VRRP groups or VRIDs on all interfaces are displayed.

If no value for vrid is specified, the statistics for all virtual routers on the specified interface are displayed.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show vrrp statistics** command:

```
Router# show vrrp statistics
Invalid packets:
  Invalid checksum:                 0
  Unknown/unsupported versions:     3
  Invalid vrID:                     1
  Too short:                        7
Protocol:
  Transitions to Master             4
Packets:
  Total received:                   54
  Adverts sent:                     0
  Bad TTL:                          0
  Short Packets:                    6
  Failed authentication:            0
  Unknown authentication:           2
```

```
Conflicting authentication:          0
Unknown Type field:                  1
Conflicting Advertise time:          0
Conflicting Addresses:               0
Received with zero priority:         9
Sent with zero priority:             0
```

unicast-peer

To enable IPv4 and IPv6 layer 3 unicast transport on Virtual Router Redundancy Protocol (VRRP), use the command in VRRP virtual router submode. To disable unicast transport, use the **no** form of this command.

unicast-peer { *ipv4-address* | *ipv6-link-local-addres* }

Syntax Description

ipv4-address	IPv4 address
ipv6-link-local-address	IPv6 link-local address

Command Default

VRRP transmits multicast traffic.

Command Modes

VRRP virtual router configuration

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Usage Guidelines

You can configure the unicast-peer command only once, allowing for the participation of only two physical routers in a unicast VRRP session.

When you configure the unicast-peer command, the router neither sends nor receives multicast packets

Task ID

Task ID	Operation
vrrp	read,write

Example

This example shows how to configure IPv4 Layer 3 unicast transport on VRRP.

```
Router(config)# router vrrp
Router(config-vrrp)# interface GigabitEthernet0/0/0/0
Router(config-vrrp-if)# address-family ipv4
Router(config-vrrp-address-family)# vrrp 1

Router(config-vrrp-virtual-router)# address 10.0.1.100

Router(config-vrrp-virtual-router)# unicast-peer 10.0.1.1
```

This example shows how to configure IPv6 Layer 3 unicast transport on VRRP.

```
Router(config)# router vrrp
Router(config-vrrp)# interface GigabitEthernet0/0/0/0
Router(config-vrrp-if)# address-family ipv6
Router(config-vrrp-address-family)# vrrp 2

Router(config-vrrp-virtual-router)# unicast-peer FE80::260:3EFF:FE11:6770
```