Cisco IOS XR IP Addresses and Services Command Reference

Cisco IOS XR Software Release 3.5

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

Text Part Number: OL-12275-01

Cisco IOS XR IP Addresses and Services Command Reference

Preface

The *Cisco IOS XR IP Addresses and Services Command Reference* contains commands related to IP addresses and services features.

The preface contains the following sections:

Changes to This Document

Table 1 lists the technical changes made to this document since it was first printed.

Table 1 Changes to This Document

Revision	Date	Change Summary
OL-12275-01	June 2007	Initial release of this document.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Access List Commands on Cisco IOS XR Software

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

An access control list (ACL) consists of one or more access control entries (ACEs) that collectively define the network traffic profile. This profile can then be referenced by Cisco IOS XR software features such as traffic filtering, priority or custom queueing, and dynamic access control. Each ACL includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

For detailed information about ACL concepts, configuration tasks, and examples, see the *Cisco IOS XR IP Addresses and Services Configuration Guide*.

clear access-list ipv4

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

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

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 2147483646.
hardware	Identifies the access list as an access group for an interface.
ingress	Specifies an inbound direction.
egress	Specifies an outbound direction.
interface	(Optional) Clears the interface statistics.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	(Optional) Clears hardware resource counters from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
sequence *number*	(Optional) Clears counters for an access list with a specific sequence number. Range is 1 to 2147483646.

Defaults

The default clears the specified IPv4 access list.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The range for the *sequence-number* argument was changed from 2147483646 to 2147483644. The command name was changed from **clear ipv4 access-list** to **clear access-list ipv4**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The **interface** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 the **hardware** keyword to clear counters for an access list that was enabled using the **ipv4 access-group** command.

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

Note An access list can be shared among multiple interfaces. Clearing hardware counters clears all counters for all interfaces that use the specified access list in a given direction (ingress or egress).

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:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255 any (51 matches)
  20 permit ip 172.16.0.0 0.0.255.255 any (26 matches)
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30 (5 matches)

RP/0/RP0/CPU0:router# clear access-list ipv4 marketing

RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
```

```
  10 permit ip 192.168.34.0 0.0.0.255 any
  20 permit ip 172.16.0.0 0.0.255.255 any
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30
```

In the following example, counters for an access list named acl_hw_1 in the outbound direction are cleared:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
  10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
  20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
  30 deny tcp any any (58 hw matches)

RP/0/RP0/CPU0:router# clear access-list ipv4 acl_hw_1 hardware egress location 0/2/cp0

RP/0/RP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
  10 permit icmp 192.168.36.0 0.0.0.255 any
  20 permit ip 172.16.3.0 0.0.255.255 any
  30 deny tcp any any
```

Related Commands

Command	Description
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
resequence access-list ipv4	Renumbers an existing statement and increments subsequent statements to allow a new IPv4 access list statements.

clear access-list ipv6

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

clear access-list ipv6 *access-list-name* [*sequence-number* | **hardware** {**ingress** | **egress**}] [**interface** *type instance*] [**location** *node-id* | **sequence** *number*]

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.
hardware	Identifies the access list as an access group for an interface.
ingress	Specifies an inbound direction.
egress	Specifies an outbound direction.
interface	(Optional) Clears the interface statistics.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	Clears counters for an access list enabled on a card interface. The *node-id* argument is entered in the rack/slot/module notation.
sequence *number*	(Optional) Specifies a specific sequence number that clears access list counters. Range is 1 to 2147483644.

Defaults

The default clears the specified IPv6 access list.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The range for the *sequence-number* argument was changed from 2147483646 to 2147483644. The command name was changed from **clear ipv6 access-list** to **clear access-list ipv6**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The **interface** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 the **hardware** keyword to clear counters for an access list that was enabled using the **ipv6 access-group** command.

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

Note An access list can be shared among multiple interfaces. Clearing hardware counters clears all counters for all interfaces that use the specified access list in a given direction (ingress or egress).

Task ID

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

Examples

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

```
RP/0/RP0/CPU0:router# show access-lists ipv6 marketing

ipv6 access-list marketing
  10 permit ipv6 3333:1:2:3::/64 any (51 matches)
  20 permit ipv6 4444:1:2:3::/64 any (26 matches)
  30 permit ipv6 5555:1:2:3::/64 any (5 matches)

RP/0/RP0/CPU0:router# clear access-list ipv6 marketing
```

```
RP/0/RP0/CPU0:router# show access-lists ipv6 marketing

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
```

In the following example, counters for an access list named acl_hw_1 in the outbound direction are cleared:

```
RP/0/RP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
  10 permit ipv6 3333:1:2:3::/64 any (251 hw matches)
  20 permit ipv6 4444:1:2:3::/64 any (29 hw matches)
  30 deny tcp any any (58 hw matches)

RP/0/RP0/CPU0:router# clear access-list ipv6 acl_hw_1 hardware egress location 0/2/cp0

RP/0/RP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
  10 permit ipv6 3333:1:2:3::/64 any
  20 permit ipv6 4444:1:2:3::/64 any
  30 deny tcp any any
```

Related Commands

Command	Description
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

copy access-list ipv4

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **copy ipv4 access-list** to **copy access-list ipv4**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 list-1

ipv4 access-list list-1
  10 permit tcp any any log
  20 permit ip any any
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RP0/CPU0: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:

```
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list

RP/0/RP0/CPU0:router# show access-lists ipv4 list-3

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

Related Commands

Command	Description
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

copy access-list ipv6

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

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.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **copy ipv6 access-list** to **copy access-list ipv6**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

```
RP/0/RP0/CPU0:router# show access-lists ipv6 list-1

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

RP/0/RP0/CPU0:router# copy access-list ipv6 list-1 list-2
RP/0/RP0/CPU0:router# show access-lists ipv6 list-2

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

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

```
RP/0/RP0/CPU0:router# copy access-list ipv6 list-1 list-3

list-3 exists in access-list

RP/0/RP0/CPU0:router# show access-lists ipv6 list-3

ipv6 access-list list-3
  10 permit ipv6 any any
  20 deny tcp any any log
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

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), 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*] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**ttl** *ttl value1 value2*]

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** | **log-input**] [**icmp-off**]

Internet Group Management Protocol (IGMP)

[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] [**fragments**] [**log** | **log-input**]

Stream Control Transmission Protocol (SCTP)

[*sequence-number*] **deny sctp** *source source-wildcard* [*operator* {*port* | *protocol-port*}] *destination destination-wildcard* [*operator* {*port* | *protocol-port*}] [**established**] [**ack**] [**rst**] [**syn**] [**fin**] [**psh**] [**urg**] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]

Transmission Control Protocol (TCP)

[*sequence-number*] **deny tcp** *source source-wildcard* [*operator* {*port* | *protocol-port*}] *destination destination-wildcard* [*operator* {*port* | *protocol-port*}] [**established**] | {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]

User Datagram Protocol (UDP)

[*sequence-number*] **deny udp** *source source-wildcard* [*operator* {*port* | *protocol-port*}] *destination destination-wildcard* [*operator* {*port* | *protocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]

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 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list** command to change the number of the first statement and increment subsequent statements of a configured access list.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use 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**, **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **pcp**, **sctp**, **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, SCTP, and TCP allow further qualifiers, which are described later in this table.
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: • **match**–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.
packet-length operator	(Optional) Packet length operator used for filtering.

packet-length value	(Optional) Packet length used to match only packets in the range of the length.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list 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 logging message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
ttl value1 value2	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value1* 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-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. 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 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	(Required) For the TCP protocol **match-any**, **match-all**. Flag names are: ack, fin, psh, rst, syn.

Defaults

There is no specific condition under which a packet is denied passing the IPv4 access list.

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Release	Modification
Release 3.3.0	The optional keywords **match-any** and **match-all** were added for the TCP protocol. The argument *flag-name* was added for the TCP protocol. The **match-any** and **match-all** keywords and the *flag-name* argument are supported on the Cisco CRS-1. The optional keyword **icmp-off** was added for the ICMP protocol.
Release 3.4.0	The optional keyword **ttl** and the associated arguments *ttl value1* and *value2* and *operator,* with range values, were added to the command.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 **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.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the **resequence access-list** command to renumber the first statement and increment the entry number of each subsequent statement. The *increment* argument causes new, unused line numbers between statements. Then add a new statement with the *entry-number* argument, specifying where it belongs in the access list.

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 deny condition for an access list named Internetfilter:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets the permit conditions for an IPv4 access list
remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
resequence access-list ipv4	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

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*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log**] [**log-input**] [**ttl** *operator ttl value1 value2*]

no *sequence-number*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **deny icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*icmp-type*] [*icmp-code*] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**log**] [**log-input**] [**icmp-off**]

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

[*sequence-number*] **deny udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**log**] [**log-input**]

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 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list** command to change the number of the first statement and increment subsequent statements of a configured access list.
protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **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.
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.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches non-initial 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.
packet-length operator	(Optional) Packet length operator used for filtering.
packet-length value	(Optional) Packet length used to match only packets in the range of the length.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was 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 logging message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
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).
ttl value1 value2	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value1* 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-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	(Required) For the TCP protocol **match-any**, **match-all**. Flag names are: ack, fin, psh, rst, syn.

Defaults

No IPv6 access list is defined.

ICMP message generation is enabled by default.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The optional keywords **match-any** and **match-all** were added for the TCP protocol. The argument *flag-name* was added for the TCP protocol. The **match-any** and **match-all** keywords and the *flag-name* argument are supported on the Cisco CRS-1. The optional keyword **icmp-off** was added for the ICMP protocol.
Release 3.4.0	The optional keyword **ttl** and the associated arguments *ttl value1, value2* and *operator,* with range values, were added to the command.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

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.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to configure the IPv6 access list named toCISCO and applies the access list to outbound traffic on Packet-over-SONET (POS) interface 0/2/0/2. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry in the list keeps all packets that have a source UDPo port number less than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of

POS interface 0/2/0/2. The second permit entry in the list permits all other traffic to exit out of POS interface 0/2/0/2. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list toCISCO
RP/0/RP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit any any
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group tOCISCO out
```

Related Commands

Command	Description
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
resequence access-list ipv6	Changes the starting entry number of the first statement in an existing IPv6 access list, and the number by which subsequent statements are incremented.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

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**} [**hardware-count**] [**interface-statistics**]

no ipv4 access-group *access-list-name* {**ingress | egress**} [**hardware-count**] [**interface-statistics**]

Syntax Description

access-list-name	Name of an IPv4 access list as specified by an **ipv4 access-list** command.
ingress	Filters on inbound packets.
egress	Filters on outbound packets.
hardware-count	(Optional) Specifies to access a group's hardware counters.
interface-statistics	(Optional) Specifies per-interface statistics in the hardware.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The keywords {**in** | **out**} were changed to {**ingress** | **egress**}.
Release 3.3.0	No modification.
Release 3.4.0	The argument *hw-count* was changed to *hardware-count*.
Release 3.5.0	The **interface-statistics** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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. Use the **ingress** keyword to filter on inbound packets or the **egress** keyword to filter on outbound packets. Use the *hardware-count* argument to enable hardware counters for the access group.

Permitted packets are counted only when hardware counters are enabled using the *hardware-count* argument. Denied packets are counted whether hardware counters are enabled or not.

Note For packet filtering applications using the **ipv4 access-group** command, packet counters are maintained in hardware for each direction. If an access group is used on multiple interfaces in the same direction, then packets are counted for each interface that has the *hardware-count* argument enabled.

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 inbound and outbound from Packet-over-SONET (POS) interface 0/2/0/2:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-egress-filter egress
```

The following example shows how to apply per-interface statistics in the hardware:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
interface-statistics
```

Related Commands

Command	Description
clear access-list ipv4	Resets the IPv4 access list match counters.
deny (IPv4)	Sets the deny conditions for an IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets the permit conditions for an IPv4 access list
show access-lists ipv4	Displays the contents of all current IPv4 access lists.
show ipv4 interface	Displays the usability status of interfaces configured for IPv4.

ipv4 access-list

To define an IPv4 access list by name, use the **ipv4 access-list** command in global configuration 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.

Defaults

No IPv4 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 **resequence access-list ipv4** command if you want to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv4 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

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

Task ID

Task ID	Operations
acl	read, write

Examples

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

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-if)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-if)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-if)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(config-if)# 39 remark Block BGP traffic from 172.16 net.
RP/0/RP0/CPU0:router(config-if)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
range 1300 1400
```

Related Commands

Command	Description
clear access-list ipv4	Resets the IPv4 access list match counters.
deny (IPv4)	Sets the deny conditions for a named IPv4 access list.
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
permit (IPv4)	Sets the permit conditions for a named IPv4 access list.
remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
resequence access-list ipv4	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

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 global configuration 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.

Defaults

Default is 1.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:.

```
RP/0/RP0/CPU0: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 global configuration 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.

Defaults

For IPv4 access lists, 2147483647 updates are logged.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

Related Commands

Command	Description
deny (IPv4)	Sets the deny conditions for an IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets the permit conditions for an IPv4 access list
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

ipv4 access-list maximum ace threshold

To set the maximum number of access control entries (ACEs) for IPv4 access lists, use the **ipv4 access-list maximum ace threshold** command in global configuration mode. To reset the ACE limit for IPv4 access lists, use the **no** form of this command.

ipv4 access-list maximum ace threshold *ace-number*

no ipv4 access-list maximum ace threshold *ace-number*

Syntax Description

ace-number	Maximum number of configurable ACEs allowed. Range is 200000 to 350000.

Defaults

200000 ACEs are allowed for IPv4 access lists.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv4 access-list maximum ace threshold** command to set the maximum number of configurable ACEs for IPv4 access lists. Out of resource (OOR) limits the number of ACEs that can be configured in the system. When the maximum number of configurable ACEs is reached, configuration of new ACEs is rejected.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to set the maximum number of ACEs for IPv4 access lists to 205000:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list maximum ace threshold 205000
```

Related Commands

Command	Description
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

ipv4 access-list maximum acl threshold

To set the maximum number of configurable IPv4 access control lists (ACLs), use the **ipv4 access-list maximum acl threshold** command in global configuration mode. To reset the IPv4 ACL limit, use the **no** form of this command.

ipv4 access-list maximum acl threshold *acl-number*

no ipv4 access-list maximum ace threshold *acl-number*

Syntax Description

acl-number	Maximum number of configurable ACLs allowed. Range is 5000 to 9000.

Defaults

5000 IPv4 ACLs can be configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv4 access-list maximum acl threshold** command to set the maximum number of configurable IPv4 ACLs. Out of resource (OOR) limits the number of ACLs that can be configured in the system. When the maximum number of configurable ACLs is reached, configuration of new ACLs is rejected.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to set the maximum number of configurable IPv4 ACLs to 6500:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list maximum acl threshold 6500
```

Related Commands

Command	Description
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

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**} [**interface-statistics**]

no ipv6 access-group *access-list-name* {**ingress** | **egress**} [**interface-statistics**]

Syntax Description

access-list-name	Name of an IPv6 access list as specified by an **ipv6 access-list** command.
ingress	Filters on inbound packets.
egress	Filters on outbound packets.
interface-statistics	(Optional) Specifies per-interface statistics in the hardware.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The keywords {**in**	**out**} were changed to {**ingress**	**egress**}.
Release 3.4.0	No modification.
Release 3.5.0	The **interface-statistics** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Use the **ipv6 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* to specify a particular IPv6 access list. Use the **in** keyword to filter on inbound packets or the **out** keyword to filter on outbound packets.

Note For packet filtering applications using the **ipv6 access-group** command, packet counters are maintained in hardware for each direction. If an access group is used on multiple interfaces in the same direction, then packets are counted for each interface.

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 a rate-limited 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
ipv6	read, write

Examples

The following example shows how to apply filters on packets inbound and outbound from Packet-over-SONET (POS) interface 0/2/0/2:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group p-out-filter egress
```

The following example shows how to apply per-interface statistics in the hardware:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress
interface-statistics
```

Related Commands

Command	Description
copy access-list ipv6	Copies an existing IPv6 access list.
deny (IPv6)	Sets the deny conditions for an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets conditions under which a packet passes a named IPv6 access list.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.
show ipv6 interface	Displays the status and configuration for a specified interface including the inbound and outbound access-lists that are applied to the interface.

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 global 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.

Defaults

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 global configuration 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.

Refer to the **deny (IPv6)** and **permit (IPv6)** commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. See the “Examples” section for an example of a translated IPv6 access control list (ACL) configuration.

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.

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

The following example shows how to configure the IPv6 access list named list2 and applies the ACL to outbound traffic on interface Packet-over-SONET (POS) 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 POS 0/2/0/2. The second entry in the ACL permits all other traffic to exit out of interface POS 0/2/0/2. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list list2
RP/0/RP0/CPU0:router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 20 permit any any

RP/0/RP0/CPU0:router# show ipv6 access-lists list2

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

RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group list2 out
```

Note IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration 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).

Related Commands

Command	Description
deny (IPv6)	Sets the deny conditions for an IPv6 access list.
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

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 global configuration 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.

Defaults

Default is 1.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

```
RP/0/RP0/CPU0: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 global configuration 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.

Defaults

For IPv6 access lists, 350000 updates are logged.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list log-update threshold 10
```

Related Commands

Command	Description
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

ipv6 access-list maximum ace threshold

To set the maximum number of access control entries (ACEs) for IPv6 access lists, use the **ipv6 access-list maximum ace threshold** command in global configuration mode. To reset the ACE limit for IPv6 access lists, use the **no** form of this command.

ipv6 access-list maximum ace threshold *ace-number*

no ipv6 access-list maximum ace threshold *ace-number*

Syntax Description

ace-number	Maximum number of configurable ACEs allowed. Range is 50000 to 350000.

Defaults

50,000 ACEs are allowed for IPv6 access lists.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	Range was 50000 to 100000 changed to 50000 to 350000.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv6 access-list maximum ace threshold** command to set the maximum number of configurable ACEs for IPv6 access lists. Out of resource (OOR) limits the number of ACEs that can be configured in the system. When the maximum number of configurable ACEs is reached, configuration of new ACEs is rejected.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

The following example shows how to set the maximum number of ACEs for IPv6 access lists to 75000:

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list maximum ace threshold 75000
```

Related Commands

Command	Description
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

ipv6 access-list maximum acl threshold

To set the maximum number of configurable IPv4 access control lists (ACLs), use the **ipv6 access-list maximum acl threshold** command in global configuration mode. To reset the IPv6 ACL limit, use the **no** form of this command.

ipv6 access-list maximum acl threshold *acl-number*

no ipv6 access-list maximum ace threshold *acl-number*

Syntax Description

acl-number	Maximum number of configurable ACLs allowed. Range is 1000 to 16000.

Defaults

1000 IPv6 ACLs can be configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	Maximum range was changed from 2000 to 16000.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv6 access-list maximum acl threshold** command to set the maximum number of configurable IPv6 ACLs. Out of resource (OOR) limits the number of ACLs that can be configured in the system. When the limit is reached, configuration of new ACLs is rejected.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

The following example shows how to set the maximum number of configurable IPv6 ACLs to 1500:

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list maximum acl threshold 1500
```

Related Commands

Command	Description
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

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), 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*] [**default nexthop** [*ipv4-address1*] [*ipv4-address2*] [*ipv4-address3*]] [**dscp** *dscp*] [**fragments**] [*packet-length operator packet-length value*] [**log** | **log-input**] [**nexthop** [*ipv4-address1*] [*ipv4-address2*] [*ipv4-address3*]] [**ttl** *ttl 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**] [**log** | **log-input**] [**icmp-off**]

Internet Group Management Protocol (IGMP)

[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] [**fragments**] [**log** | **log-input**]

Stream Control Transmission Protocol (SCTP)

[*sequence-number*] **permit sctp** *source source-wildcard* [*operator* {*port* | *protocol-port*}] *destination destination-wildcard* [*operator* {*port* | *protocol-port*}] [**established**] [**ack**] [**rst**] [**syn**] [**fin**] [**psh**] [**urg**] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]

Transmission Control Protocol (TCP)

[*sequence-number*] **permit tcp** *source source-wildcard* [*operator* {*port* | *protocol-port*}] *destination destination-wildcard* [*operator* {*port* | *protocol-port*}] [**established**] | {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]

User Datagram Protocol (UDP)

[*sequence-number*] **permit udp** *source source-wildcard* [*operator* {*port* | *protocol-port*}] *destination destination-wildcard* [*operator* {*port* | *protocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] [**fragments**] [**log** | **log-input**]

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 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list** command to change the number of the first statement and increment subsequent statements of a configured access list.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use 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**, **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **pcp**, **sctp**, **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, SCTP, and TCP allow further qualifiers, which are described later in this table.
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: • **match**–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)
default nexthop	(Optional) Specifies the default next hop for this entry. If the **default nexthop** keyword is configured, ACL-based forwarding action is taken only if the results of the PLU lookup for the destination of the packets determine a default route; that is, no specified route is determined to the destination of the packet.
ipv4-address1 *ipv4-address2* *ipv4-address3*	(Optional) Uses one to three next-hop addresses. The IP address types are defined as follows: • Default IP addresses—Specifies the next-hop router in the path toward the destination in which the packets must be forwarded, if there is no explicit route for the destination address of the packet in the routing table. The first IP address that is associated with a connected interface that is currently up is used to route the packets. • Specified IP addresses—Specifies the next-hop router in the path toward the destination in which the packets must be forwarded. The first IP address that is associated with a connected interface that is currently up is used to route the packets.

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 non-initial fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.
packet-length operator	(Optional) Packet length operator used for filtering.
packet-length value	(Optional) Packet length used to match only packets in the range of the length.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list 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 logging message also includes the input interface.

nexthop	(Optional) Forwards the specified next hop for this entry.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
ttl value1 value2	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value1* 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-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. 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	(Required) For the TCP protocol **match-any**, **match-all**. Flag names are: ack, fin, psh, rst, syn.

Defaults

There is no specific condition under which a packet is denied passing the IPv4 access list.

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The optional keywords **match-any** and **match-all** were added for the TCP protocol. The argument *flag-name* was added for the TCP protocol. The **match-any** and **match-all** keywords and the *flag-name* argument are supported on the Cisco CRS-1. The optional keyword **icmp-off** was added for the ICMP protocol.
Release 3.4.0	The optional keyword **ttl** and the associated arguments *ttl value1, value2,* and *operator,* with range values, were added to the command.
Release 3.4.1	Both the **default nexthop** and **nexthop** keywords were added to support ACL-based forwarding on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the **resequence access-list** command to renumber the first statement and increment the entry number of each subsequent statement. The *increment* argument causes new, unused line numbers between statements. Then add a new statement with the *entry-number* specifying where it belongs in the access list.

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.

For ACL-based forwarding, we recommend that you use the **permit** command and **any any** keywords for the last ACL-based forwarding ACE rule to overwrite an implicit deny of security ACL. It ensures that all packets are forwarded with the traditional destination IP address if you do not want to drop any non-ABF related packets.

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:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 permit tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

The following example shows how to configure ACL-based forwarding with security for an access list configuration:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list security-abf-acl
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 10.0.0.0 0.255.255.255 any
RP/0/RP0/CPU0:router(config-ipv4-acl)# 15 permit ipv4 30.2.0.0 0.0.255.255 any nexthop
40.1.1.2
```

```
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny ipv4 30.1.0.0 0.0.255.255 any
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 permit ipv4 30.0.0.0 0.255.255.255 any
```

The following example shows how to configure a pure ACL-based forwarding:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list security-abf-acl
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit ipv4 10.0.0.0 0.255.255.255 any nexthop
50.1.1.2
RP/0/RP0/CPU0:router(config-ipv4-acl)# 15 permit ipv4 30.2.1.0 0.0.0.255 any
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit ipv4 30.2.0.0 0.0.255.255 any nexthop
40.1.1.2
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 permit ipv4 any any
```

Related Commands

Command	Description
deny (IPv4)	Sets the conditions for an IPv4 access list.
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
resequence access-list ipv4	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

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** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [*packet-length operator packet-length value*] [**log**] [**log-input**] [**ttl** *operator ttl value1 value2*]

no *sequence-number*

Internet Control Message Protocol (ICMP)

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

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

[*sequence-number*] **permit udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* {*port* | *protocol-port*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* {*port* | *protocol-port*}] [**dscp** *value*] [**routing**] [**authen**] [**destopts**] [**fragments**] [**log**] [**log-input**]

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 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the **resequence access-list** command to change the number of the first statement and increment subsequent statements of a configured access list.
protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length	Source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.

host *source-ipv6-address*	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.
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 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 to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	Specifies the destination IPv6 host address about which to set permit conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
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.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches non-initial 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.
packet-length operator	(Optional) Packet length operator used for filtering.
packet-length value	(Optional) Packet length used to match only packets in the range of the length.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
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).
ttl value1 value2	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value1* 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-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.
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.

Defaults

No IPv6 access list is defined.

ICMP message generation is enabled by default.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The optional keywords **match-any** and **match-all** were added for the TCP protocol. The argument *flag-name* was added for the TCP protocol. The **match-any** and **match-all** keywords and the *flag-name* argument are supported on the Cisco CRS-1. The optional keyword **icmp-off** was added for the ICMP protocol.
Release 3.4.0	The optional keyword **ttl** and the associated arguments *ttl value1, value2,* and *operator,* with range values, were added to the command.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 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 applies the access list to outbound traffic on Packet-over-SONET (POS) interface 0/2/0/2. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry in the list keeps all packets that have a source

UDP port number less than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of POS interface 0/2/0/2. The second permit entry in the list permits all other traffic to exit out of POS interface 0/2/0/2. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list toCISCO
RP/0/RP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit any any
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group tOCISCO out
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
resequence access-list ipv6	Changes the starting entry number of the first statement in an existing IPv6 access list, and the number by which subsequent statements are incremented.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

remark (IPv4)

To write a helpful comment (remark) for an entry in an IPv4 access list, use the **remark** command in IPv4 access list configuration mode. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483646. (By default, the first statement is number 10; subsequent statements are incremented by 10.)
remark	Comment that describes the entry in the access list, up to 255 characters long.

Defaults

The IPv4 access list entries have no remarks.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **remark** command to write a helpful comment for an entry in an IPv4 access list. To remove the remark, use the **no** form of this command.

The remark can be up to 255 characters; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Use the **resequence access-list ipv4** command if you want to add statements to an existing access list and the sequence numbers of consecutive entries do not permit additional statements.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

In the following example, the user1 subnet is not allowed to use outbound Telnet:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RP0/CPU0:router# show ipv4 access-list telnetting

ipv4 access-list telnetting
  0 remark Do not allow user1 to telnet out
  20 deny tcp 172.16.2.88 255.255.0.0 any eq telnet out
  30 permit icmp any any
```

Related Commands

Command	Description
deny (IPv4)	Sets the deny conditions for an IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets the permit conditions for an IPv4 access list
resequence access-list ipv4	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark** command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
remark	Comment that describes the entry in the access list, up to 255 characters long.

Defaults

The IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Use the **remark** command to write a helpful comment for an entry in an IPv6 access list. To remove the remark, use the **no** form of this command.

The remark can be up to 255 characters; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Use the **resequence access-list ipv6** command if you want to add statements to an existing access list and the sequence numbers of consecutive entries do not permit additional statements.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, a remark is added:

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 3333:1:2:3::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 20 permit ipv6 4444:1:2:3::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 30 permit ipv6 5555:1:2:3::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 39 remark Block BGP traffic from a given host
RP/0/RP0/CPU0:router(config-ipv6-acl)# 40 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
RP/0/RP0/CPU0:router# show ipv6 access-list Internetfilter

ipv6 access-list Internetfilter
  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
  39 remark Block BGP traffic from a given host
  40 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1400
```

Related Commands

Command	Description
deny (IPv6)	Sets the deny conditions for an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets permit conditions for an IPv6 access list
resequence access-list ipv6	Changes the starting entry number of the first statement in an existing IPv6 access list, and the number by which subsequent statements are incremented.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

resequence access-list ipv4

To renumber existing statements and increment subsequent statements to allow a new IPv4 access list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence access-list ipv4** command in EXEC mode.

resequence access-list ipv4 *name* [*base* [*increment*]]

Syntax Description

name	Name of an IPv4 access list.
base	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483644. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644. Default is 10.

Defaults

base: 10
increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **resequence ipv4 access-list** to **resequence access-list ipv4**. The *increment* maximum value was changed from 2147483646 to 2147483644.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **resequence access-list ipv4** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv4 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, suppose you have an existing access list:

```
ipv4 access-list marketing
  1 permit 10.1.1.1
  2 permit 10.2.0.0 0.0.255.255
  3 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

You want to add additional entries in the access list. First you resequence the entries, renumbering the statements starting with number 20 and an increment of 5, and then you have room for four additional statements between each of the existing statements:

```
RP/0/RP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

Now you add your new entries.

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  3 remark Do not allow user1 to telnet out
  4 deny tcp host 171.69.2.88 255.255.0.0 any eq telnet
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  29 remark Allow user2 to telnet out
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

Related Commands

Command	Description
deny (IPv4)	Sets the deny conditions for an IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets the permit conditions for an IPv4 access list
remark (IPv4)	Inserts a helpful remark about an IPv4 access list. entry
show access-lists ipv4	Displays the contents of all current IPv4 access lists.

resequence access-list ipv6

To renumber existing statements and increment subsequent statements to allow a new IPv6 access list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence access-list ipv6** command in EXEC mode.

resequence access-list ipv6 *name* [*base* [*increment*]]

Syntax Description

name	Name of an IPv6 access list.
base	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483646. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644. Default is 10.

Defaults

base: 10
increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.The command name was changed from **resequence ipv6 access-list** to **resequence access-list ipv6**. The *increment* maximum value was changed from 2147483646 to 2147483644.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Use the **resequence access-list ipv6** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv6 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, suppose you have an existing access list:

```
ipv6 access-list Internetfilter
  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
```

You want to add additional entries in the access list. First, you resequence the entries, renumbering the statements starting with number 20 and an increment of 5, and then you have room for four additional statements between each of the existing statements:

```
RP/0/RP0/CPU0:router# resequence access-list ipv6 Internetfilter 20 5
RP/0/RP0/CPU0:router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
  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
```

Now you add your new entries.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv6-acl)# 3 remark Block BGP traffic from a given host
RP/0/RP0/CPU0:router(config-ipv6-acl)# 4 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
RP/0/RP0/CPU0: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
```

Related Commands

Command	Description
deny (IPv6)	Sets the deny conditions for an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Set permit conditions for an IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
show access-lists ipv6	Displays the contents of all current IPv6 access lists.

show access-lists ipv4

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

show access-lists ipv4 [*access-list-name* **hardware** {**ingress | egress**} [**interface** *type instance*] {**sequence** *number* **| location** *node-id*} **| summary** [*access-list-name*] **|** *access-list-name* [*sequence-number*] **| maximum** [**detail**] [**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	Identifies the access list as an access list for an interface.
ingress	Specifies an inbound interface.
egress	Specifies an outbound interface.
sequence *number*	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483646.
interface	(Optional) Displays interface statistics.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	Location of a particular IPv4 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483646.

maximum	Displays the current maximum number of configurable IPv4 access control lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	Displays the packet filtering usage for the specified line card.

Defaults

The default displays all IPv4 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **show ipv4 access-lists** to **show access-lists ipv4**.
Release 3.3.0	The optional keywords **usage** and **pfilter** were added.
Release 3.4.0	No modification.
Release 3.4.1	Sample output fields were updated to support ACL-based forwarding as an ingress-only feature on the Cisco CRS-1.
Release 3.5.0	The **interface** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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** or **egress**, 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 (ingress or egress). 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-lists ipv4 maximum detail** command to display the OOR details for IPv4 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

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:

```
RP/0/RP0/CPU0:router# show access-lists ipv4

ipv4 access-list 101
  10 deny udp any any eq ntp
  20 permit tcp any any
  30 permit udp any any eq tftp
  40 permit icmp any any
  50 permit udp any any eq domain
ipv4 access-list Internetfilter
  10 permit tcp any 172.16.0.0 0.0.255.255 eq telnet
  20 deny tcp any any
  30 deny udp any 172.18.0.0 0.0.255.255 lt 1024
  40 deny ipv4 any any log
```

In the following example, the contents of an access list named Internetfilter are displayed to show an example of ACL-based forwarding:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 Internetfilter

ipv4 access-list Internetfilter
  10 permit ipv4 host 50.3.3.3 any nexthop 1.1.1.1 2.2.2.2 3.3.3.3
  20 permit ipv4 host 50.60.1.2 any nexthop 50.70.1.2 50.80.1.2
  25 permit ipv4 host 50.2.2.2 any nexthop 50.70.1.2
  30 permit ipv4 host 50.70.1.2 any nexthop 50.80.1.2
  40 permit ipv4 host 1.1.1.1 any nexthop 50.70.1.2
  50 permit ipv4 host any any
```

In the following example, the contents of an access list named acl_hw_1 are displayed to show an example of ACL-based forwarding for the brief **hardware** option:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware ingress location 0/1/cpu0

ipv4 access-list ucode
 10 permit ipv4 host 50.3.3.3 any
 20 permit ipv4 host 50.60.1.2 any (661765 hw matches) (next-hop: 50.70.1.2)
 25 permit ipv4 host 50.2.2.2 any (next-hop: 50.70.1.2)
 30 permit ipv4 host 50.70.1.2 any (next-hop: 50.80.1.2)
 40 permit ipv4 host 1.1.1.1 any (next-hop: 50.70.1.2)
 50 permit ipv4 host 9.9.9.9 any
```

In the following example, the contents of an access list named acl_hw_1 are displayed to show an example of ACL-based forwarding for a specific access list entry for the hardware **detail** option:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware ingress sequence 20 detail
location 0/1/CPU0

ACL name: ucode
Sequence Number: 20
Grant: permit
Logging: OFF
Per ace icmp: ON
Next Hop Enable: ON <<<<<<<<< (ABF specific)
Next-hop: 50.70.1.2 <<<<<<<<< (ABF specific)
Default Next Hop: OFF<<<<<<<<< (ABF specific)
Hits: 661765
Statistics pointer: 0x60016
```

```
Number of TCAM entries: 1


Entry : 0 for ACE : 20
RAW value  : 0x00000040 0xffffffff 0xffffff11 0x0000007f 0xfdf2ffff 0xffffffff
RAW mask   : 0x000000ff 0xfc000000 0x000000ff 0x00000080 0xffff0000 0000000000
RAW result : 0x00000000 0x00000003 0x00000000 0x01010101

------------------------------Field Details---------------------------------
acl_id             : 0x03f
acl_id mask        : 0x3ff
```

In the following example, the contents of an access list named acl_hw_1 are displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
  10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
  20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
  30 deny tcp any any (58 hw matches)
```

Table 2 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.
next-hop	Next hop is programmed and is reachable through FIB.
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.
Next Hop Enable	When the ABF next hop is configured on an ACE, the Next Hop Enable is set to on.
Default Next Hop	When the ABF default-next-hop is configured in an ACE, the Default Next Hop is set to on.
Hits	Hardware counter for that ACE.
Statistics pointer	Statistics pointer is the pointer that is assigned for hardware counters.
Number of TCAM entries	Number of TCAM entries that are used to program the ACE into hardware.

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

```
RP/0/RP0/CPU0:router# show access-lists ipv4 summary

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

Table 3 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.

In the following example, the OOR details of the IPv4 access lists are displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 maximum detail

Default max configurable acls :5000
Default max configurable aces :200000
Current configured acls       :1
Current configured aces       :2
Current max configurable acls :5000
Current max configurable aces :200000
Max configurable acls         :9000
Max configurable aces         :350000
```

Table 4 describes the significant fields shown in the display.

Table 4 show access-lists ipv4 maximum detail Field Descriptions

Field	Description
Default max configurable acls	Default maximum number of configurable IPv4 ACLs allowed.
Default max configurable aces	Default maximum number of configurable IPv4 ACEs allowed.
Current configured acls	Number of configured IPv4 ACLs.
Current configured aces	Number of configured IPv4 ACEs.
Current max configurable acls	Configured maximum number of configurable IPv4 ACLs allowed.
Current max configurable aces	Configured maximum number of configurable IPv4 ACEs allowed.
Max configurable acls	Maximum number of configurable IPv4 ACLs allowed.
Max configurable aces	Maximum number of configurable IPv4 ACEs allowed.

Related Commands

Command	Description
clear access-list ipv4	Resets the IPv4 access list match counters.
copy access-list ipv4	Copies an existing IPv4 access list.
deny (IPv4)	Sets the deny conditions for an IPv4 access list.
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets the permit conditions for an IPv4 access list
remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
resequence access-list ipv4	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.

show access-lists ipv6

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

show access-lists ipv6 [*access-list-name* **hardware** {**ingress | egress**} [**interface** *type instance*] {**sequence** *number* | **location** *node-id*} | **summary** [*access-list-name*] | *access-list-name* [*sequence-number*] | **maximum** [**detail**] [**usage** {**pfilter 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.
hardware	Identifies the access list as an access list for an interface.
ingress	Specifies an inbound interface.
egress	Specifies an outbound interface.
sequence *number*	(Optional) Sequence number of a particular IPv6 access list. Range is 1 to 2147483646.
interface	(Optional) Displays interface statistics.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	Location of a particular IPv4 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	Displays a summary of all current IPv6 access lists.
sequence-number	(Optional) Sequence number of a particular IPv6 access list. Range is 1 to 2147483646.

maximum	Displays the current maximum number of configurable IPv6 access control lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.
usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	Displays the packet filtering usage for the specified line card.

Defaults

Displays all IPv6 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **show ipv6 access-lists** to **show access-lists ipv6**.
Release 3.3.0	The optional keywords **usage** and **pfilter** were added.
Release 3.4.0	No modification.
Release 3.5.0	The **interface** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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** or **egress**, 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 (ingress or egress). 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-lists ipv6 maximum detail** command to display the OOR details for IPv6 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

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 IPv6 access lists are displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv6

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
ipv6 access-list marketing
  10 permit ipv6 7777:1:2:3::/64 any (51 matches)
  20 permit ipv6 8888:1:2:3::/64 any (26 matches)
  30 permit ipv6 9999:1:2:3::/64 any (5 matches)
```

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

```
RP/0/RP0/CPU0: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
```

In the following example, the contents of an access list named acl_hw_1 is displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
  10 permit icmp any any (251 hw matches)
  20 permit ipv6 3333:1:2:3::/64 any (29 hw matches)
  30 deny tcp any any (58 hw matches)
```

Table 5 describes the significant fields shown in the display.

Table 5 show access-lists ipv6 hardware Field Descriptions

Field	Description
hw matches	Number of hardware matches.

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

```
RP/0/RP0/CPU0:router# show access-lists ipv6 summary

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

Table 6 describes the significant fields shown in the display.

Table 6 show access-lists ipv6 summary 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:

```
RP/0/RP0/CPU0: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
```

Table 7 describes the significant fields shown in the display.

Table 7 show access-lists pv6 maximum detail Field Descriptions

Field	Description
Default max configurable acls	Default maximum number of configurable IPv6 ACLs allowed.
Default max configurable aces	Default maximum number of configurable IPv6 ACEs allowed.
Current configured acls	Number of configured IPv6 ACLs.
Current configured aces	Number of configured IPv6 ACEs.
Current max configurable acls	Configured maximum number of configurable IPv6 ACLs allowed.
Current max configurable aces	Configured maximum number of configurable IPv6 ACEs allowed.
Max configurable acls	Maximum number of configurable IPv6 ACLs allowed.
Max configurable aces	Maximum number of configurable IPv6 ACEs allowed.

Related Commands

Command	Description
copy access-list ipv6	Copies an existing IPv6 access list.
deny (IPv6)	Sets the deny conditions for an IPv6 access list.
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Set permit conditions for an IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
resequence access-list ipv6	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.

ARP Commands on Cisco IOS XR Software

This chapter describes the commands used to configure and monitor the Address Resolution Protocol (ARP).

arp

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration 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.

Defaults

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added. The encapsulation information was added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 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:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# arp 192.168.7.19 0800.0900.1834 arpa
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show arp	Displays the ARP cache.

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

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

Defaults

Default value is off.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0/RP1/CPU0/0
RP/0/RP0/CPU0:router(config-if)# arp purge-delay 50
```

arp timeout

To specify how long 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.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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)# interface MgmtEth 0/RP1/CPU0/0
RP/0/RP0/CPU0:router(config-if)# arp timeout 3600
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show arp	Displays the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the networking device. **Note** See the *Cisco IOS XR Interface and Hardware Component Command Reference* for information on using the **show interfaces** command.

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 EXEC mode.

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

Syntax Description

traffic	(Optional) Deletes traffic statistics on the specified interface.
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 (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.
location *node-id*	Clears the ARP entries for a specified location. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **location** keyword and *node-id* argument were made mandatory.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# clear arp-cache traffic gigabitEthernet 0/1/5/1 location 0/1/CPU0
```

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

```
RP/0/RP0/CPU0:router# clear arp-cache location 0/1/CPU0
```

Related Commands

Command	Description
arp	Adds a permanent entry in the ARP cache.
show arp	Displays the ARP cache.

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 arguments or keywords.

Defaults

Proxy ARP is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 MgmtEth interface 0/RP1/CPU0/0:

```
RP/0/RP0/CPU0:router(config)# interface MgmtEth 0/RP1/CPU0/0
RP/0/RP0/CPU0:router(config-if)# proxy-arp
```

show arp

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

show arp [**vrf** *vrf-name*] [*ip-address* [**location** *node-id*] | *hardware-address* [**location** *node-id*] | **traffic** [**location** *node-id* | *interface-instance*]

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.
location *node-id*	(Optional) Displays the ARP entry for a specific location. The *node-id* argument is entered in the *rack/slot/module* notation.
hardware-address	(Optional) The ARP entries that match the 48-bit MAC address are displayed.
traffic	(Optional) Displays ARP traffic statistics.
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 (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.

Defaults

The active RP is the default location.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show arp

-------------------------------------------------------------------------------
0/3/CPU0
-------------------------------------------------------------------------------

Address         Age        Hardware Addr   State      Type  Interface
192.4.1.1       -          000c.cfe6.3336  Interface  ARPA GigabitEthernet0/3/1/3
192.4.1.2       01:37:50   0000.c004.0102  Dynamic    ARPA GigabitEthernet0/3/1/3
2.1.4.2         -          000c.cfe6.33b5  Interface  ARPA FastEthernet0/3/3/4
2.1.0.2         -          000c.cfe6.33b1  Interface  ARPA FastEthernet0/3/3/0
2.1.0.1         00:37:56   000a.8b08.857a  Dynamic    ARPA FastEthernet0/3/3/0
2.1.4.1         01:37:51   000a.8b08.857e  Dynamic    ARPA FastEthernet0/3/3/4
211.11.1.1      -          000c.cfe6.32fa  Interface  ARPA FastEthernet0/3/0/6
2.1.5.2         -          000c.cfe6.33b6  Interface  ARPA FastEthernet0/3/3/5
2.1.1.2         -          000c.cfe6.33b2  Interface  ARPA FastEthernet0/3/3/1
2.1.1.1         01:37:51   000a.8b08.857b  Dynamic    ARPA FastEthernet0/3/3/1
2.1.5.1         01:37:50   000a.8b08.857f  Dynamic    ARPA FastEthernet0/3/3/5

-------------------------------------------------------------------------------
0/2/CPU0
-------------------------------------------------------------------------------
Address         Age        Hardware Addr   State      Type  Interface
5.6.9.1         01:11:55   0003.fe4c.0bff  Dynamic    ARPA MgmtEth0/2/CPU0/0
5.6.25.6        01:09:29   000c.cfe6.2000  Dynamic    ARPA MgmtEth0/2/CPU0/0
5.6.5.10        00:39:58   0009.7b49.0bff  Dynamic    ARPA MgmtEth0/2/CPU0/0
```

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

```
RP/0/RP0/CPU0:router# show arp MgmtEth 0/RP1/CPU0/0
```

```
Address         Age        Hardware Addr   State      Type  Interface
10.4.9.2        00:35:55   0030.7131.abfc  Dynamic    ARPA  MgmtEth0/RP1/CPU0/0
10.4.9.1        00:35:55   0000.0c07.ac24  Dynamic    ARPA  MgmtEth0/RP1/CPU0/0
10.4.9.99       00:49:12   0007.ebea.44d0  Dynamic    ARPA  MgmtEth0/RP1/CPU0/0
10.4.9.199      -          0001.c9eb.dffe  Interface  ARPA  MgmtEth0/RP1/CPU0/0
```

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

```
RP/0/RP0/CPU0:router# show arp 0005.5f1d.8100

Address Age Hardware Addr State Type Interface
172.16.7.2 - 0005.5f1d.8100 Interface ARPA GigabitEthernet2/0/1/2
```

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

```
RP/0/RP0/CPU0: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
172.16.7.1 00:35:49 0002.fc0e.9600 Dynamic ARPA GigabitEthernet2/0/1/2
172.16.7.2 - 0005.5f1d.8100 Interface ARPA GigabitEthernet2/0/1/2
```

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

```
RP/0/RP0/CPU0:router# show arp traffic

ARP statistics:
  Recv: 2691 requests, 91 replies
  Sent: 67 requests, 2 replies (0 proxy, 1 gratuitous)
  Resolve requests rcvd: 1
  Resolve requests dropped: 0
  Errors: 0 out of memory, 0 no buffers

ARP cache:
  Total ARP entries in cache: 4
  Dynamic: 3, Interface: 1, Standby: 0
  Alias: 0,   Static: 0

  IP Packet drop count for node 0/0/CPU0: 1
```

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

```
RP/0/RP0/CPU0:router# show arp traffic location 0/2/CPU0

ARP statistics:
Recv: 0 requests, 1 replies
Sent: 0 requests, 2 replies (0 proxy, 2 gratuitous)
Resolve requests rcvd: 0
Resolve requests dropped: 0
Errors: 0 out of memory, 0 no buffers

ARP cache:
Total ARP entries in cache: 4
Dynamic: 1, Interface: 1, Static: 1
Alias: 1, Standby: 0

  IP Packet drop count for node 0/2/CPU0: 1
```

Table 8 describes the significant fields shown in the display.

Table 8 show arp 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 • Standby (for HSRP) • Incomplete • "-" (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.
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*.

Related Commands

Command	Description
arp	Adds a permanent entry to the ARP cache.
clear arp-cache	Deletes all dynamic entries from the ARP cache.

Cisco Express Forwarding Commands on Cisco IOS XR Software

This chapter describes the commands used to configure and monitor Cisco Express Forwarding (CEF) on Cisco IOS XR software.

For detailed information about CEF concepts, configuration tasks, and examples, see *Cisco IOS XR IP Addresses and Services Configuration Guide*.

clear adjacency ipv4

To clear the IPv4 CEF adjacency table, use the **clear adjacency ipv4** command in EXEC mode.

clear adjacency statistics ipv4 [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Clears the IPv4 CEF adjacency table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you issue the **clear adjacency statistics ipv4** command, entries in the adjacency table that reside on the route processor (RP) are removed and then repopulated.

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

Task ID

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

Examples

The following example shows how to clear the IPv4 CEF adjacency table on the RP:

```
RP/0/RP0/CPU0:router# clear adjacency statistics ipv4
```

Related Commands

Command	Description
show adjacency	Displays the IPv4 CEF adjacency table.

clear adjacency statistics

To clear adjacency packet and byte counter statistics, use the **clear adjacency statistics** command in 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 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.
location *node-id*	(Optional) Clears detailed adjacency statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	Supplemented *Examples* section to include additional show output.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This 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

Examples

The following example displays sample output of the Cisco Express Forwarding (CEF) adjacency table information, and clears the IPv4 CEF adjacency statistics:

```
RP/0/RP0/CPU0:router# show adjacency detail

------------------------------------------------------------------------------
0/RP1/CPU0
------------------------------------------------------------------------------
Interface                  Address                Version  Refcount  Protocol
MgmtEth0/RP1/CPU0/0         (src mac only)              1         1     ipv4
                           000000000000001193efe8fe0800
                           mtu: 1500, flags 1 0 1
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         (interface)                 2         1
                           (interface entry)
                           flags 1 0 4
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.77               29         2     ipv4
                           001193efe8e2001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.105              19         2     ipv4
                           001b2a4e53e5001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.241              18         2     ipv4
                           001819d18c38001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.173              15         2     ipv4
                           0015c75f09f8001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.81                9         2     ipv4
                           001a6c40d89c001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.1                 6         2     ipv4
                           0030f2f21038001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           1 packets, 60 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.201               3         2     ipv4
                           00107b3c6847001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.96               23         2     ipv4
                           0018ba800c80001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.168              22         2     ipv4
                           00503ee3dd80001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.152              21         2     ipv4
                           00503ee3df40001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.180              16         2     ipv4
                           0015c75f0800001193efe8fe0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0         172.29.52.28               12         2     ipv4
                           00127fd6ba09001193efe8fe0800
```

```
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.76            7         2     ipv4
                        001193efe8ea001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.200           4         2     ipv4
                        00107b3c689f001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.83           26         2     ipv4
                        001a6c40d89c001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.151          25         2     ipv4
                        000a41052e01001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.91           17         2     ipv4
                        0018742c5f40001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.127          14         2     ipv4
                        0013c4cba200001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.27           11         2     ipv4
                        00127fd6ba08001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.75            8         2     ipv4
                        001193efe8e2001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.182          27         2     ipv4
                        0015c75f0800001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.150          24         2     ipv4
                        000a41052da1001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.90           20         2     ipv4
                        001874163f80001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.70           13         2     ipv4
                        5a5900000201001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.82           10         2     ipv4
                        00127fd6bc36001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP1/CPU0/0      172.29.52.126           5         2     ipv4
                        0013c4cba548001193efe8fe0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
------------------------------------------------------------------------------
0/RP0/CPU0
------------------------------------------------------------------------------
Interface                Address                Version  Refcount  Protocol
MgmtEth0/RP0/CPU0/0      (src mac only)             2         1     ipv4
                        0000000000005a59000002010800
```

```
                        mtu: 1500, flags 1 0 1
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      (interface)                  1         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.77                38        2      ipv4
                        001193efe8e25a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.105               29        2      ipv4
                        001b2a4e53e55a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.241               28        2      ipv4
                        001819d18c385a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.173               24        2      ipv4
                        0015c75f09f85a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.81                19        2      ipv4
                        001a6c40d89c5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.13                16        2      ipv4
                        001079e960385a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.153               15        2      ipv4
                        00e0b0552cc45a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.121               13        2      ipv4
                        0012da0b97ff5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.1                  6        2      ipv4
                        0030f2f210385a59000002010800
                        mtu: 1500, flags 1 0 0
                        257909 packets, 9246567 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.201                4        2      ipv4
                        00107b3c68475a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.96                32        2      ipv4
                        0018ba800c805a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.168               31        2      ipv4
                        00503ee3dd805a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.152               30        2      ipv4
                        00503ee3df405a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.180               25        2      ipv4
                        0015c75f08005a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.28                22        2      ipv4
                        00127fd6ba095a59000002010800
```

```
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.76           17         2      ipv4
                        001193efe8ea5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.52           14         2      ipv4
                        0090929c88485a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.148          12         2      ipv4
                        00b064fce0bb5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.120          10         2      ipv4
                        00042892c7ff5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.200           5         2      ipv4
                        00107b3c689f5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.83           35         2      ipv4
                        001a6c40d89c5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.151          34         2      ipv4
                        000a41052e015a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.91           27         2      ipv4
                        0018742c5f405a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.127          23         2      ipv4
                        0013c4cba2005a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.27           21         2      ipv4
                        00127fd6ba085a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.75           18         2      ipv4
                        001193efe8e25a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.51           11         2      ipv4
                        00e04f5fe0685a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.71            3         2      ipv4
                        001193efe8fe5a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.182          36         2      ipv4
                        0015c75f08005a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.150          33         2      ipv4
                        000a41052da15a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.90           26         2      ipv4
                        001874163f805a59000002010800
```

```
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.82                20         2     ipv4
                        00127fd6bc365a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.50                 9         2     ipv4
                        0090929cf8685a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.190                8         2     ipv4
                        00000c4775e05a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
MgmtEth0/RP0/CPU0/0      172.29.52.126                7         2     ipv4
                        0013c4cba5485a59000002010800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
------------------------------------------------------------------------------
0/6/CPU0
------------------------------------------------------------------------------
Interface                Address                Version  Refcount  Protocol
GigabitEthernet0/6/5/7    (src mac only)                4         1     ipv4
                        00000000000000000c07fa5e0800
                        mtu: 1500, flags 1 0 1
                        0 packets, 0 bytes
POS0/6/4/0                (interface)                  27         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
POS0/6/0/0                (interface)                  26         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
GigabitEthernet0/6/5/7    (interface)                  25         1
                        (interface entry)
                        flags 1 0 4
                        47 packets, 1974 bytes
GigabitEthernet0/6/5/1    (src mac only)                6         1     ipv4
                        00000000000000000c015cb80800
                        mtu: 1500, flags 1 0 1
                        222195 packets, 19973644 bytes
GigabitEthernet0/6/5/2    (src mac only)                5         1     ipv4
                        00000000000000000c02c9d60800
                        mtu: 1500, flags 1 0 1
                        222251 packets, 19978582 bytes
GigabitEthernet0/6/5/6    (interface)                  24         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
GigabitEthernet0/6/5/5    (interface)                  23         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
GigabitEthernet0/6/5/4    (interface)                  22         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
GigabitEthernet0/6/5/3    (interface)                  21         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
GigabitEthernet0/6/5/2    (interface)                  20         1
                        (interface entry)
```

```
                                flags 1 0 4
                                12001 packets, 2155986 bytes
GigabitEthernet0/6/5/1           (interface)                  19          1
                                (interface entry)
                                flags 1 0 4
                                10803 packets, 1717298 bytes
GigabitEthernet0/6/5/0           (interface)                  18          1
                                (interface entry)
                                flags 1 0 4
                                0 packets, 0 bytes
POS0/6/0/3                       (interface)                  32          1
                                (interface entry)
                                flags 1 0 4
                                0 packets, 0 bytes
POS0/6/4/2                       (interface)                  31          1
                                (interface entry)
                                flags 1 0 4
                                0 packets, 0 bytes
POS0/6/0/1                       (src mac only)               43          1     ipv4
                                0f000800
                                mtu: 4470, flags 1 0 1
                                222207 packets, 17752538 bytes
POS0/6/0/1                       point to point               42          2     ipv4
                                0f000800
                                mtu: 4470, flags 1 0 0
                                0 packets, 0 bytes
POS0/6/0/1                       point to point               41          2     mpls
                                0f008847
                                mtu: 4470, flags 1 0 0
                                0 packets, 0 bytes
POS0/6/0/2                       (interface)                  30          1
                                (interface entry)
                                flags 1 0 4
                                0 packets, 0 bytes
POS0/6/4/1                       (interface)                  29          1
                                (interface entry)
                                flags 1 0 4
                                0 packets, 0 bytes
POS0/6/0/1                       (interface)                  28          1
                                (interface entry)
                                flags 1 0 4
                                73519 packets, 3019532 bytes
POS0/6/4/6                       (src mac only)               48          1     ipv4
                                0f000800
                                mtu: 4470, flags 1 0 1
                                222198 packets, 17751798 bytes
POS0/6/4/6                       point to point               47          2     ipv4
                                0f000800
                                mtu: 4470, flags 1 0 0
                                0 packets, 0 bytes
POS0/6/4/6                       point to point               46          2     mpls
                                0f008847
                                mtu: 4470, flags 1 0 0
                                0 packets, 0 bytes
POS0/6/4/7                       (interface)                  40          1
                                (interface entry)
                                flags 1 0 4
                                0 packets, 0 bytes
POS0/6/4/6                       (interface)                  39          1
                                (interface entry)
                                flags 1 0 4
                                72915 packets, 2918638 bytes
POS0/6/4/5                       (src mac only)               45          1     ipv4
                                0f000800
```

```
                        mtu: 4470, flags 1 0 1
                        0 packets, 0 bytes
POS0/6/4/5               point to point               44         2     ipv4
                        0f000800
                        mtu: 4470, flags 1 0 0
                        0 packets, 0 bytes
POS0/6/4/4               (src mac only)               51         1     ipv4
                        0f000800
                        mtu: 4470, flags 1 0 1
                        222198 packets, 17751852 bytes
POS0/6/4/4               point to point               50         2     ipv4
                        0f000800
                        mtu: 4470, flags 1 0 0
                        0 packets, 0 bytes
POS0/6/4/4               point to point               49         2     mpls
                        0f008847
                        mtu: 4470, flags 1 0 0
                        0 packets, 0 bytes
POS0/6/4/5               (interface)                  35         1
                        (interface entry)
                        flags 1 0 4
                        66317 packets, 1458970 bytes
POS0/6/4/4               (interface)                  34         1
                        (interface entry)
                        flags 1 0 4
                        72306 packets, 2799786 bytes
POS0/6/4/3               (interface)                  33         1
                        (interface entry)
                        flags 1 0 4
                        0 packets, 0 bytes
GigabitEthernet0/6/5/2    10.16.8.6                   11         2     mpls
                        0013c4cba4a200000c02c9d68847
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
GigabitEthernet0/6/5/2    10.16.8.6                   10         2     ipv4
                        0013c4cba4a200000c02c9d60800
                        mtu: 1500, flags 1 0 0
                        19693 packets, 1143510 bytes
GigabitEthernet0/6/5/1    10.12.20.2                   8         2     mpls
                        00156358bc6c00000c015cb88847
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
GigabitEthernet0/6/5/1    10.12.20.2                   7         2     ipv4
                        00156358bc6c00000c015cb80800
                        mtu: 1500, flags 1 0 0
                        19806 packets, 1153348 bytes
GigabitEthernet0/6/5/7    10.12.40.2                   9         2     ipv4
                        00156358bc7200000c07fa5e0800
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
------------------------------------------------------------------------------
0/4/CPU1
------------------------------------------------------------------------------
Interface                 Address                Version  Refcount  Protocol
SBC2                                                3         2     ipv6
                        ::
                        00000000
                        mtu: 1500, flags 1 0 0
                        0 packets, 0 bytes
                        (externally managed adj)
                        Client id : 0x985
                        Client dll : libsvii_adj_pd.dll
                        Client completion function : svii_adj_cmpl_adj
SBC2                     point to point               2         2     ipv4
```

```
                          00000000
                          mtu: 1500, flags 1 0 0
                          0 packets, 0 bytes
                          (externally managed adj)
                          Client id : 0x985
                          Client dll : libsvii_adj_pd.dll
                          Client completion function : svii_adj_cmpl_adj
MgmtEth0/4/CPU1/0          (interface)                  1         1
                          (interface entry)
                          flags 1 0 4
                          0 packets, 0 bytes
------------------------------------------------------------------------------
0/4/CPU0
------------------------------------------------------------------------------
Interface                  Address                Version  Refcount  Protocol
SBC1                                                   8         2     ipv6
                          ::
                          00000000
                          mtu: 1500, flags 1 0 0
                          0 packets, 0 bytes
                          (externally managed adj)
                          Client id : 0x985
                          Client dll : libsvii_adj_pd.dll
                          Client completion function : svii_adj_cmpl_adj
SBC1                       point to point               9         2     ipv4
                          00000000
                          mtu: 1500, flags 1 0 0
                          0 packets, 0 bytes
                          (externally managed adj)
                          Client id : 0x985
                          Client dll : libsvii_adj_pd.dll
                          Client completion function : svii_adj_cmpl_adj
MgmtEth0/4/CPU0/0          (interface)                  1         1
                          (interface entry)
                          flags 1 0 4
                          0 packets, 0 bytes
------------------------------------------------------------------------------
0/1/CPU0
------------------------------------------------------------------------------
Interface                  Address                Version  Refcount  Protocol
Bundle-POS24               point to point             119         2     mpls
                          0f008847
                          mtu: 4470, flags 80000001 0 50000000
                          0 packets, 0 bytes
                          (externally managed adj)
                          Client id : 0x5ee
                          Client dll : libbundlemgr_cmpl_pi.dll
                          Client completion function : bma_cmpl_adj
Bundle-Ether28.1           (src mac only)             149         1     ipv4
                          000000000000001563c0b0f68100001d0800
                          mtu: 1500, flags 80000001 0 50000001
                          0 packets, 0 bytes
                          (externally managed adj)
                          Client id : 0x5ee
                          Client dll : libbundlemgr_cmpl_pi.dll
                          Client completion function : bma_cmpl_adj
Bundle-Ether28.2           (src mac only)             148         1     ipv4
                          000000000000001563c0b0f68100001e0800
                          mtu: 1500, flags 80000001 0 50000001
                          0 packets, 0 bytes
                          (externally managed adj)
                          Client id : 0x5ee
                          Client dll : libbundlemgr_cmpl_pi.dll
                          Client completion function : bma_cmpl_adj
```

```
Bundle-Ether28.3            (src mac only)              147         1     ipv4
                            00000000000001563c0b0f68100001f0800
                            mtu: 1500, flags 80000001 0 50000001
                            0 packets, 0 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
Bundle-Ether28              (src mac only)              146         1     ipv4
                            00000000000001563c0b0f60800
                            mtu: 1500, flags 80000001 0 50000001
                            0 packets, 0 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
Bundle-POS24                (src mac only)              121         1     ipv4
                            0f000800
                            mtu: 4470, flags 80000001 0 50000001
                            34 packets, 2712 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
Bundle-POS24                point to point              120         2     ipv4
                            0f000800
                            mtu: 4470, flags 80000001 0 50000000
                            2 packets, 106 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
GigabitEthernet0/1/5/1      (src mac only)               13         1     ipv4
                            00000000000001563c0b0f10800
                            mtu: 1500, flags 1 0 1
                            310470 packets, 27909626 bytes
GigabitEthernet0/1/5/2      (src mac only)               12         1     ipv4
                            00000000000001563c0b0f20800
                            mtu: 1500, flags 1 0 1
                            310468 packets, 27909354 bytes
Bundle-Ether28.1            (interface)                 139         1
                            (interface entry)
                            flags 80000001 0 50001004
                            66 packets, 3036 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
Bundle-Ether28.2            (interface)                 142         1
                            (interface entry)
                            flags 80000001 0 50001004
                            66 packets, 3036 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
Bundle-Ether28.3            (interface)                 145         1
                            (interface entry)
                            flags 80000001 0 50001004
                            66 packets, 3036 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
```

```
Bundle-Ether28               (interface)                 136         1
                            (interface entry)
                            flags 80000001 0 50001004
                            264 packets, 11880 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
Bundle-POS24                 (interface)                 118         1
                            (interface entry)
                            flags 80000001 0 50001004
                            10627 packets, 2210404 bytes
                            (externally managed adj)
                            Client id : 0x5ee
                            Client dll : libbundlemgr_cmpl_pi.dll
                            Client completion function : bma_cmpl_adj
GigabitEthernet0/1/5/7       (interface)                  31         1
                            (interface entry)
                            flags 1 0 4
                            31063 packets, 3851812 bytes
GigabitEthernet0/1/5/6       (interface)                  30         1
                            (interface entry)
                            flags 1 0 4
                            31327 packets, 3863692 bytes
GigabitEthernet0/1/5/5       (interface)                  29         1
                            (interface entry)
                            flags 1 0 4
                            0 packets, 0 bytes
GigabitEthernet0/1/5/4       (interface)                  28         1
                            (interface entry)
                            flags 1 0 4
                            0 packets, 0 bytes
GigabitEthernet0/1/5/3       (interface)                  27         1
                            (interface entry)
                            flags 1 0 4
                            0 packets, 0 bytes
GigabitEthernet0/1/5/2       (interface)                  26         1
                            (interface entry)
                            flags 1 0 4
                            11579 packets, 2315638 bytes
GigabitEthernet0/1/5/1       (interface)                  25         1
                            (interface entry)
                            flags 1 0 4
                            17686 packets, 3081588 bytes
GigabitEthernet0/1/5/0       (src mac only)               14         1     ipv4
                            00000000000000000c00393a0800
                            mtu: 1500, flags 1 0 1
                            0 packets, 0 bytes
GigabitEthernet0/1/5/0       (interface)                  24         1
                            (interface entry)
                            flags 1 0 4
                            65 packets, 2730 bytes
POS0/1/0/0                   (interface)                  19         1
                            (interface entry)
                            flags 1 0 4
                            0 packets, 0 bytes
POS0/1/4/0                   (interface)                  18         1
                            (interface entry)
                            flags 1 0 4
                            134452 packets, 7791702 bytes
POS0/1/4/3                   (interface)                   7         1
                            (interface entry)
                            flags 1 0 4
                            0 packets, 0 bytes
```

```
POS0/1/0/2                  (interface)                  22         1
                           (interface entry)
                           flags 1 0 4
                           0 packets, 0 bytes
POS0/1/0/1                  point to point               95         2     mpls
                           0f008847
                           mtu: 4470, flags 1 0 0
                           0 packets, 0 bytes
POS0/1/0/1                  (src mac only)               97         1     ipv4
                           0f000800
                           mtu: 4470, flags 1 0 1
                           36 packets, 2874 bytes
POS0/1/0/1                  point to point               96         2     ipv4
                           0f000800
                           mtu: 4470, flags 1 0 0
                           0 packets, 0 bytes
POS0/1/4/2                  (src mac only)              110         1     ipv4
                           ff030021
                           mtu: 4470, flags 1 0 1
                           0 packets, 0 bytes
POS0/1/4/2                  point to point              109         2     ipv4
                           ff030021
                           mtu: 4470, flags 1 0 0
                           0 packets, 0 bytes
POS0/1/4/2                  (interface)                   3         1
                           (interface entry)
                           flags 1 0 4
                           191172 packets, 2294213 bytes
POS0/1/0/1                  (interface)                  21         1
                           (interface entry)
                           flags 1 0 4
                           103403 packets, 4243616 bytes
POS0/1/4/1                  (interface)                  20         1
                           (interface entry)
                           flags 1 0 4
                           123823 packets, 5581162 bytes
POS0/1/0/3                  (interface)                  23         1
                           (interface entry)
                           flags 1 0 4
                           0 packets, 0 bytes
GigabitEthernet0/1/5/1      10.14.8.4                    56         2     mpls
                           0012da0b9600001563c0b0f18847
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
GigabitEthernet0/1/5/1      10.14.8.4                    17         2     ipv4
                           0012da0b9600001563c0b0f10800
                           mtu: 1500, flags 1 0 0
                           35523 packets, 2247965 bytes
GigabitEthernet0/1/5/2      10.16.4.6                    54         2     mpls
                           0013c4cba4a1001563c0b0f28847
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes
GigabitEthernet0/1/5/2      10.16.4.6                    15         2     ipv4
                           0013c4cba4a1001563c0b0f20800
                           mtu: 1500, flags 1 0 0
                           35502 packets, 2244864 bytes
Bundle-Ether28.2            10.12.30.2                  152         2     ipv4
                           00156358b9f6001563c0b0f68100001e0800
                           mtu: 1500, flags 80000001 0 50000000
                           0 packets, 0 bytes
                           (externally managed adj)
                           Client id : 0x5ee
                           Client dll : libbundlemgr_cmpl_pi.dll
                           Client completion function : bma_cmpl_adj
```

```
Bundle-Ether28.3            10.12.31.2                  151         2     ipv4
                           00156358b9f6001563c0b0f68100001f0800
                           mtu: 1500, flags 80000001 0 50000000
                           0 packets, 0 bytes
                           (externally managed adj)
                           Client id : 0x5ee
                           Client dll : libbundlemgr_cmpl_pi.dll
                           Client completion function : bma_cmpl_adj
Bundle-Ether28              10.12.28.2                  150         2     ipv4
                           00156358b9f6001563c0b0f60800
                           mtu: 1500, flags 80000001 0 50000000
                           0 packets, 0 bytes
                           (externally managed adj)
                           Client id : 0x5ee
                           Client dll : libbundlemgr_cmpl_pi.dll
                           Client completion function : bma_cmpl_adj
Bundle-Ether28.1            10.12.29.2                  153         2     ipv4
                           00156358b9f6001563c0b0f68100001d0800
                           mtu: 1500, flags 80000001 0 50000000
                           0 packets, 0 bytes
                           (externally managed adj)
                           Client id : 0x5ee
                           Client dll : libbundlemgr_cmpl_pi.dll
                           Client completion function : bma_cmpl_adj
GigabitEthernet0/1/5/0      10.12.16.2                   16         2     ipv4
                           00156358b9f000000c00393a0800
                           mtu: 1500, flags 1 0 0
                           0 packets, 0 bytes

RP/0/RP0/CPU0:router# clear adjacency statistics ipv4
```

Related Commands

Command	Description
show adjacency	Displays the IPv4 CEF adjacency table.

clear cef ipv4 drops

To clear CEF IPv4 packet drop counters, use the **clear cef ipv4 drops** command in EXEC mode.

clear cef ipv4 drops [**location** *node-id*]

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 shows how to clear IPv4 CEF drop counters for location 0/1/CPU0:

```
RP/0/RP0/CPU0:router# clear cef ipv4 drops location 0/1/CPU0

   Node: 0/1/CPU0
   Clearing CEF Drop Statistics
```

Related Commands

Command	Description
show cef ipv4 drops	Displays IPv4 packet drop counters.

clear cef ipv4 exceptions

To clear IPv4 CEF exception packet counters, use the **clear cef ipv4 exceptions** command in EXEC 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 shows how to clear IPv4 CEF exception packets for all nodes:

```
RP/0/RP0/CPU0:router# clear cef ipv4 exceptions location 0/1/CPU0

Node: 0/1/CPU0
Clearing CEF Exception Statistics
```

Related Commands

Command	Description
show cef ipv4 exceptions	Displays IPv4 CEF exception packet counters.

clear cef ipv4 interface bgp-policy-statistics

To clear CEF IPv4 interface BGP policy statistics, use the **clear cef ipv4 interface bpg-policy-statistics** command in EXEC mode.

clear cef ipv4 interface *type instance* **bpg-policy-statistics**

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.0	This command was introduced on the Cisco CRS-1.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command clears the Border Gateway Protocol (BGP) policy accounting counters for the specified interface.

Task ID

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

Examples

The following example shows how to clear IPv4 CEF BGP policy statistics:

```
RP/0/RP0/CPU0:router# clear cef ipv4 interface MgmtEth 0/RP1/CPU0/0 bgp-policy-statistics
```

Related Commands

Command	Description
show cef ipv4 interface bgp-policy-statistics	Displays IPv4 interface BGP policy statistics.

clear cef ipv4 interface rpf-statistics

To clear CEF IPv4 interface reverse path forwarding (RPF) statistics, use the **clear cef ipv4 interface rpf-statistics** command in EXEC mode.

clear cef ipv4 interface *type instance* **rpf-statistics** [**location** *node-id*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	(Optional) Clears IPv6 packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear cef ipv4 interface rpf-statistics** command clears the reverse path forwarding (RPF) counters for the specified interface.

Task ID

Task ID	Operations
cef	read

Examples

The following example shows how to clear IPv4 CEF RPF statistics for location 0/1/CPU0:

```
RP/0/RP0/CPU0:router# clear cef ipv4 interface pos 0/1/0/0 rpf-statistics location
0/1/CPU0
```

clear cef ipv6 drops

To clear CEF IPv6 packet drop counters, use the **clear cef ipv6 drop** command in EXEC mode.

clear cef ipv6 drops [**location** *node-id*]

Syntax Description

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 shows how to clear IPv6 CEF drop counters for all nodes:

```
RP/0/RP0/CPU0:router# clear cef ipv6 drops
```

Related Commands

Command	Description
show cef ipv6 drops	Displays IPv6 packet drop counters.

clear cef ipv6 exceptions

To clear IPv6 CEF exception packet counters, use the **clear cef ipv6 exceptions** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **location** keyword was made mandatory.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 shows how to clear IPv6 CEF exception packets for all nodes:

```
RP/0/RP0/CPU0:router# clear cef ipv6 exceptions
```

Related Commands

Command	Description
show cef ipv6 exceptions	Displays IPv6 CEF exception packet counters.

clear cef ipv6 interface bgp-policy-statistics

To clear CEF IPv6 interface BGP policy statistics, use the **clear cef ipv6 interface bpg-policy-statistics** command in EXEC mode.

clear cef ipv6 interface *type instance* **bpg-policy-statistics**

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear cef ipv6 interface bgp-policy-statistics** command clears the Border Gateway Protocol (BGP) policy accounting counters for the specified interface.

Task ID

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

Examples

The following example shows how to clear IPv4 CEF BGP policy statistics:

```
RP/0/RP0/CPU0:router# clear cef ipv6 interface MgmtEth 0/RP1/CPU0/0 bgp-policy-statistics
```

clear cef ipv6 interface rpf-statistics

To clear CEF IPv6 interface reverse path forwarding (RPF) statistics, use the **clear cef ipv6 interface rpf-statistics** command in EXEC mode.

clear cef ipv6 interface *type instance* **rpf-statistics** [**location** *node-id*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	(Optional) Clears IPv6 packet drop counters for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear cef ipv6 interface rpf-statistics** command clears the reverse path forwarding (RPF) counters for the specified interface.

Task ID

Task ID	Operations
cef	read

Examples

The following example shows how to clear IPv4 CEF RPF statistics:

```
RP/0/RP0/CPU0:router# clear cef ipv6 interface MgmtEth 0/RP1/CPU0/0 rpf-statistics
```

ipv4 bgp policy accounting

To enable Border Gateway Protocol (BGP) policy accounting, use the **ipv4 bgp policy accounting** command in interface configuration mode. To disable BGP policy accounting, use the **no** form of this command.

ipv4 bgp policy accounting {input | output {**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}}

no ipv4 bgp policy accounting {input | output {**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}}

Syntax Description

input	Enables BGP policy accounting policy on the ingress IPv4 unicast interface.
output	Enables BGP policy accounting policy on the egress IPv4 unicast interface.
{**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}	When you specify the ingress or egress interface, you must specify one of the following keywords: • **destination-accounting**—Enables accounting policy on the basis of the destination address. • **source-accounting**—Enables accounting policy on the basis of the source address. After specifying **destination-accounting** you can optionally specify **source-accounting**, or after specifying **source-accounting**, you can optionally specify **destination-accounting**.

Defaults

There is no BGP policy accounting.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.0	This command was introduced on the Cisco CRS-1.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you use the **no** form of the command, accounting is disabled for both the source and destination. To change accounting on either the destination or source address, reconfigure the **ipv4 bgp policy accounting** command specifying the **destination-accounting** or **source-accounting** keyword. In the following example, you want BGP policy accounting disabled on the source address after enabling source and destination address accounting earlier:

```
RP/0/RP0/CPU0:router(config-if)# ipv4 bgp policy accounting output destination-accounting
```

See the *Cisco IOS XR Routing Configuration Guide* for information about configuring a BGP policy. BGP accounting policy is based on community lists, autonomous system numbers, or autonomous system paths.

For BGP policy propagation to function, you must enable BGP.

To specify the accounting policy, the proper route policy configuration must be in place, matching specific BGP attributes using the **set traffic-index** command. In BGP router configuration mode, use the **table-policy** command to modify the accounting buckets when the IP routing table is updated with routes learned from BGP. To display accounting policy information, use the **show cef ipv4 interface bgp-policy-statistics**, **show bgp policy**, and **show ip route bgp** commands.

Task ID

Task ID	Operations
network	read, write

Examples

The following example shows how to configure BGP policy accounting:

```
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 bgp policy accounting output source-accounting
```

Related Commands

Command	Description
show bgp policy	Displays information about BGP advertisements under a proposed policy.
show cef ipv4 interface bgp-policy-statistics	Displays IPv4 CEF BGP policy statistics.
show route bgp	Displays the current routes for BGP in the RIB.
route-policy	Defines a route policy.
table-policy	Applies a routing policy to routes being installed into the routing table.

ipv4 verify unicast source reachable-via

To enable IPv4 unicast Reverse Path Forwarding (RPF) checking, use the **ipv4 verify unicast source reachable-via** command in interface configuration mode. To disable unicast RPF, use the **no** form of this command.

ipv4 verify unicast source reachable-via {**any** | **rx**} [**allow-default**] [**allow-self-ping**]

no ipv4 verify unicast source reachable-via {**any** | **rx**} [**allow-default**] [**allow-self-ping**]

Syntax Description

any	Enables loose unicast RPF checking. If loose unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table.
rx	Enables strict unicast RPF checking. If strict unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table and the output interface matches the interface on which the packet was received.
allow-default	(Optional) Enables the matching of default routes. This option applies to both loose and strict RPF.
allow-self-ping	(Optional) Enables the router to ping out an interface.This option applies to both loose and strict RPF.

Defaults

IPv4 unicast RPF is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The strict option information was added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv4 verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When strict unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received.

When loose unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address can be reached through any of the router interfaces.

Task ID

Task ID	Operations
ipv4	read, write,
network	read, write

Examples

The following example shows how to configure strict RPF on POS interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 verify unicast source reachable-via rx
```

The following example shows how to configure loose RPF on POS interface 0/0/0/1.

```
RP/0/RP1/CPU0:ios(config)# interface pos 0/0/0/1
RP/0/RP1/CPU0:ios(config-if)# ipv4 verify unicast source reachable-via any
```

Related Commands

Command	Description
ipv6 verify unicast source reachable-via any	Enables loose IPv6 unicast RPF checking.

ipv6 bgp policy accounting

To enable Border Gateway Protocol (BGP) policy accounting, use the **ipv6 bgp policy accounting** command in interface configuration mode. To disable BGP policy accounting, use the **no** form of this command.

ipv6 bgp policy accounting {input | output {**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}}

no ipv6 bgp policy accounting {input | output {**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}}

Syntax Description

input	Enables BGP policy accounting policy on the ingress IPv6 unicast interface.
output	Enables BGP policy accounting policy on the egress IPv6 unicast interface.
{**destination-accounting** [**source-accounting**] | **source-accounting** [**destination-accounting**]}	When you specify the ingress or egress interface, you must specify one of the following keywords: • **destination-accounting**—Enables accounting policy on the basis of the destination address. • **source-accounting**—Enables accounting policy on the basis of the source address. After specifying **destination-accounting**, you can optionally specify **source-accounting** or, after specifying **source-accounting**, you can optionally specify **destination-accounting**.

Defaults

There is no BGP policy accounting.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When you use the **no** form of the command, accounting is disabled for both the source and destination. To change accounting on either the destination or source address, reconfigure the **ipv6 bgp policy accounting** command, specifying the **destination-accounting** or **source-accounting** keyword. In the following example, you want BGP policy accounting disabled on the source address after enabling source and destination address accounting earlier:

```
RP/0/RP0/CPU0:router(config-if)# ipv6 bgp policy accounting output destination-accounting
```

See the *Cisco IOS XR Routing Configuration Guide* for information about configuring a BGP policy. BGP accounting policy is based on community lists, autonomous system numbers, or autonomous system paths.

For BGP policy propagation to function, you must enable BGP.

To specify the accounting policy, the proper route policy configuration must be in place matching specific BGP attributes using the **set traffic-index** command. In BGP router configuration mode, use the **table-policy** command to modify the accounting buckets when the IP routing table is updated with routes learned from BGP. To display accounting policy information, use the **show cef ipv4 interface bgp-policy-statistics, show bgp policy**, and **show ip route bgp** commands.

Task ID

Task ID	Operations
network	read, write

Examples

The following example shows how to configure BGP policy accounting:

```
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 bgp policy accounting output source-accounting
```

Related Commands

Command	Description
show bgp policy	Displays information about BGP advertisements under a proposed policy.
show cef ipv6 interface bgp-policy-statistics	Displays IPv6 CEF BGP policy statistics.
show route bgp	Displays the current routes for BGP in the RIB.
route-policy	Defines a route policy.
table-policy	Applies a routing policy to routes being installed into the routing table.

ipv6 verify unicast source reachable-via any

To enable loose IPv6 unicast Reverse Path Forwarding (RPF) checking, use the **ipv6 verify unicast source reachable-via any** command in interface configuration mode. To disable loose IPv6 unicast RPF checking, use the **no** form of this command.

ipv6 verify unicast source reachable-via {**any** | **rx**} [**allow-default**] [**allow-self-ping**]

no ipv6 verify unicast source reachable-via {**any** | **rx**} [**allow-default**] [**allow-self-ping**]

Syntax Description

any	Enables loose unicast RPF checking. If loose unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table.
rx	Enables strict unicast RPF checking. If strict unicast RPF is enabled, a packet is not forwarded unless its source prefix exists in the routing table and the output interface matches the interface on which the packet was received.
allow-default	(Optional) Enables the matching of default routes. This option applies to both loose and strict RPF.
allow-self-ping	(Optional) Enables the router to ping out an interface.This option applies to both loose and strict RPF.

Defaults

Loose IPv6 unicast RPF is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The keywords **any**, **rx**, **allow-default**, and **allow-self-ping** were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
network	read, write
ipv6	read, write

Examples

The following example shows how to enable loose RPF checking on POS interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 verify unicast source reachable-via any
```

Related Commands

Command	Description
ipv4 verify unicast source reachable-via	Enables IPv4 unicast RPF checking.

rp mgmtethernet forwarding

To enable switching from the line card to the route processor Management Ethernet interfaces, use the **rp mgmtethernet forwarding** command in global configuration mode. To disable switching from the modular services card to the route processor Management Ethernet interfaces, use the **no** form of this command.

rp mgmtethernet forwarding

no rp mgmtethernet forwarding

Syntax Description

This command has no arguments or keywords.

Defaults

Switching is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	This command is not supported on the Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read, write

Examples

The following example shows how to enable switching from the modular services card to the RP Management Ethernet interfaces:

```
RP/0/RP0/CPU0:router(config)# rp mgmtethernet forwarding
```

show adjacency

To display CEF adjacency table information, use the **show adjacency** command in 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. **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.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show adjacency location 0/0/CPU0

Interface                  Address                 Version  Refcount  Protocol
POS0/0/1/2                 (src mac only)                6         1     ipv4
POS0/0/1/2                 point to point                7     100004
POS0/0/1/2                 (interface)                   3         1
```

The following is sample output from the **show adjacency** command with the **detail** and **location** keywords specified:

```
RP/0/RP0/CPU0:router# show adjacency ipv4 POS 0/0/0/2 detail location 0/0/CPU0

Interface                  Address                 Version  Refcount  Protocol
POS0/0/0/2                 point to point                7    100004     ipv4
                           0f000800
                           mtu: 4470, flags 0 0 40000000
                           0 packets, 0 bytes
                           0xffffffff
```

The following is sample output from the **show adjacency ipv4 nexthop** command with the **detail** and **location** keywords specified:

```
RP/0/RP0/CPU0:router: show adjacency ipv4 nexthop 10.10.10.1 detail location 0/3/CPU0

Interface                  Address                 Version  Refcount  Protocol
POS0/3/1/0             10.10.10.1                   11         6     ipv4
                           000c86f33d330800453a21c10800
                           mtu: 1500, flags 0 0 40000000
                           0 packets, 0 bytes
                           0xffffffff
```

Table 9 describes the significant fields shown in the display.

Table 9 show adjacency 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 MTU[1].
flags	Internal field.
packets	Number of packets going through the adjacency.
bytes	Number of bytes going through the adjacency.

1. MTU = maximum transmission unit

Related Commands

Command	Description
clear adjacency ipv4	Clears the IPv4 CEF adjacency table.

show cef ipv4

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

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	The sample output for the **detail** keyword is modified for a specific prefix.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4

Prefix              Next Hop            Interface
0.0.0.0/0           12.25.0.1           MgmtEth0/RP1/CPU0/0
0.0.0.0/32          broadcast
12.25.0.0/16        attached            MgmtEth0/RP1/CPU0/0
12.25.12.10/32      receive             MgmtEth0/RP1/CPU0/0
12.25.13.12/32      12.25.13.12         MgmtEth0/RP1/CPU0/0
12.25.16.11/32      12.25.16.11         MgmtEth0/RP1/CPU0/0
12.25.22.10/32      12.25.22.10         MgmtEth0/RP1/CPU0/0
12.25.26.10/32      12.25.26.10         MgmtEth0/RP1/CPU0/0
12.25.41.2/32       12.25.41.2          MgmtEth0/RP1/CPU0/0
12.25.41.5/32       12.25.41.5          MgmtEth0/RP1/CPU0/0
12.25.42.5/32       12.25.42.5          MgmtEth0/RP1/CPU0/0
12.25.44.15/32      12.25.44.15         MgmtEth0/RP1/CPU0/0
12.25.55.2/32       12.25.55.2          MgmtEth0/RP1/CPU0/0
12.25.255.255/32    12.25.255.255       MgmtEth0/RP1/CPU0/0
224.0.0.0/4         0.0.0.0
224.0.0.1/32        0.0.0.0
255.255.255.255/32  broadcast
```

Table 10 describes the significant fields shown in the display.

Table 10 show cef ipv4 Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

The following sample output is from the **show cef ipv4** command for the **detail** keyword, 10.10.10.0/24 as the IPv4 prefix mask, and the location is 0/3/CPU0:

```
RP/0/RP0/CPU0:router# show cef ipv4 10.10.10.0/24 detail location 0/3/CPU0

10.10.10.0/24, version 0, attached, connected, internal 0x40000c01[2] 0x0, (0x59a4fd4c)
 local adjacency point2point
 Prefix Len 24, traffic index 0, precedence routine (0)
  gateway array reference count 1, flags 0x0, source 3, [0, type 3 flags 0x101000,
(0x5990efc4)]
   via POS0/2/0/0, 0 dependencies, class 0, weight 0
    local adjacency


    Load distribution: 0 (refcount 0)

    Hash  OK  Interface                 Address
    0     Y   POS0/2/0/0                point2point
```

Related Commands

Command	Description
show cef ipv6	Displays the IPv6 CEF table.

show cef ipv4 adjacency

To display IPv4 CEF adjacency status and configuration information, use the **show cef ipv4 adjacency** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 adjacency** [*interface-type interface-instance*] [**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-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 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.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

```
RP/0/RP1/CPU0:ios# show cef ipv4 adjacency MgmtEth 0/RP1/CPU0/0


Display protocol is ipv4
Interface    Address                                          Type    Refcount

Mg0/RP1/CPU0/0Prefix: 12.25.0.3/32                             local   2
              Adjacency: PT:0x782a2900 12.25.0.3/32
              Interface: Mg0/RP1/CPU0/0
              MAC: 00.d0.02.75.ab.fd.00.11.93.ef.e3.50.08.00
              Interface Type: 0x8, Base Flags: 0x1
              Dependent adj type: remote
              Dependent adj intf: Mg0/RP1/CPU0/0

Mg0/RP1/CPU0/0Prefix: 0.24.0.32/32                             remote  6
              Adjacency: PT:0x782a2b58
              Interface: Mg0/RP1/CPU0/0
              MAC: 28.4e.4f.4e.45.29
              Interface Type: 0x8, Base Flags: 0x0
```

Table 11 describes the significant fields shown in the display.

Table 11 show cef ipv4 adjacency 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.

Related Commands

Command	Description
show cef ipv6 adjacency	Displays CEF IPv6 adjacency status and configuration information.

show cef ipv4 adjacency hardware

To display IPv4 CEF adjacency hardware status and configuration information, use the **show cef ipv4 adjacency hardware** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 adjacency hardware** {**egress** | **ingress** [**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 packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

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

```
RP/0/RP0/CPU0:router# show cef ipv4 adjacency hardware

Interface    Address                                          Type    Refcount

Mg0/RP0/CPU0/0                                                 special 4
             Interface: Mg0/RP0/CPU0/0 Type:  glean
             Interface Type: 0x8, Base Flags: 0x4400
             Dependent adj type: remote
             Dependent adj intf: Mg0/RP0/CPU0/0


Mg0/RP0/CPU0/0Prefix: 64.102.12.47/32                          local   3
             Adjacency: PT:0x78f5c708 64.102.12.47/32
             Interface: Mg0/RP0/CPU0/0
             MAC: 00.30.f2.f2.10.38.00.11.93.ef.e8.e6.08.00
             Interface Type: 0x8, Base Flags: 0x1
             Dependent adj type: remote
             Dependent adj intf: Mg0/RP0/CPU0/0
```

Table 12 describes the significant fields shown in the display.

Table 12 show cef ipv4 adjacency hardware 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.

Related Commands

Command	Description
show cef ipv6 adjacency hardware	Displays IPv6 CEF adjacency hardware status and configuration information

show cef ipv4 drops

To display IPv4 CEF table packet drop counters, use the **show cef ipv4 drops** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/0/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
```

Table 13 describes the significant fields shown in the display.

Table 13 show cef ipv4 drop Field Descriptions

Field	Description
Unresolved drops	Drops due to unresolved routes.
Unsupported drops	Drops due to an unsupported feature.
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.

1. RPF = Reverse Path Forwarding

Related Commands

Command	Description
clear cef ipv4 drops	Clears IPv4 CEF packet drop counters.
clear cef ipv6 drops	Clears IPv6 CEF packet drop counters.

show cef ipv4 exact-route

To display an IPv4 CEF exact route, use the **show cef ipv4 exact-route** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 exact-route** {*source-address destination-address*} [**detail** | **location** *node-id*]

Syntax Description

vrf	(Optional) Displays 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.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

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

```
RP/0/RP0/CPU0:router# show cef ipv4 exact-route 10.1.1.1 10.1.1.2 detail

0.0.0.0/0, version 432, proxy default, internal 0x2000201[1]
 Prefix Len 0, traffic index 0, precedence routine (0)
   via MgmtEth0/RP1/CPU0/0
```

Table 14 describes the significant fields shown in the display.

Table 14 show cef ipv4 exact-route Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table.
Next Hop	Next hop of the prefix
Interface	Interface associated with the prefix

Related Commands

Command	Description
clear cef ipv4 exceptions	Displays IPv4 CEF exception packet counters.

show cef ipv4 exceptions

To display IPv4 CEF exception packet counters, use the **show cef ipv4 exceptions** command in EXEC mode.

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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/0/CPU0
  Slow encap  packets :               0
  Redirect    packets :               0
  Receive     packets :          306404
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0
Node: 0/1/CPU0
  Slow encap  packets :               0
  Redirect    packets :               0
  Receive     packets :               0
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0
Node: 0/2/CPU0
  Slow encap  packets :               0
  Redirect    packets :               0 Receive     packets :               0
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :             314
  Fragmented  packets :               0
Node: 0/3/CPU0
  Slow encap  packets :               0
  Redirect    packets :               0
  Receive     packets :               0
  Broadcast   packets :               0
  IP options  packets :               0
  TTL expired packets :               0
  Fragmented  packets :               0
```

Table 15 describes the significant fields shown in the display.

Table 15 show cef ipv4 exceptions Field Descriptions

Field	Description
Slow encap	Number of packets requiring special processing during encapsulation.
Redirect	Number of ICMP[1] 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[2].
Fragmented	Number of packets that have been fragmented.

1. ICMP = internet control message protocol
2. TTL = time to live

Related Commands

Command	Description
clear cef ipv4 exceptions	Clears IPv4 CEF exception packet counters.
clear cef ipv6 exceptions	Clears IPv6 CEF exception packet counters.

show cef ipv4 external hardware

To display information related to IPv4 CEF external clients, use the **show cef ipv4 external hardware** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 external hardare** {**ingress** | **detail**} **location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
ingress	Display information read from the ingress packet switch exchange (PSE).
detail	Displays full information about CEF external clients.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show cef ipv4 external hardware** command displays every prefix that an external client is interested in as well as the hardware information from the platform.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output for the **show cef ipv4 external hardare** command:

```
RP/0/RP0/CPU0:router# show cef vrf_1 external hardare ingress location 0/1/0

Client Name       : l2fib_mgr
Interest type     : EOS0 LDI updates
Prefix            : 3.3.3.3/32
Number of notifs  : 1
State             : resolved, mismatch, cached plat context, in retry
Via               : drop

    Load distribution: 0 (refcount 0)

    Hash  OK  Interface                Address
    0     Y   Unknown                  drop

    INGRESS External CLient Load info:
Total Recursive Paths 0
    TLU1 0x00004610 nexthop: 0.0.0.0
    TLU1 ENTRY        0
     SW: 0x00000002 00010000 00000000 00000100
     HW: 0x00000002 00010000 00000000 00000100
    local:                0x0    drop:               0x1
    next ptr:     0x00010000
    num of entries:    1
    Recursive next-hop:   0.0.0.0
```

Table 16 describes the significant fields shown in the display.

Table 16 show cef ipv4 external hardware Field Descriptions

Field	Description
Client Name	Process name of the client (for example, l2fib_mgr).
Interest type	Client interest type, which may be: • IP reachability notify • EOS0 LDI updates • IP LDI updates • 6VPE MPLS nexthop reachability • 6VPE IP tunnel nexthop reachability
Prefix	Client prefix. If the interest type is 6VPE, you will see Tunnel Id for the outgoing tunnel if the prefix length is not 0.
Number of notifs	Number of times the client has been notified about this prefix.
State	Client state, which may be: • resolved/unresolved • mismatch • path • notif pending • cached plat context • in retry • stale
Via	Next hop for this prefix.

Table 16 show cef ipv4 external hardware Field Descriptions (continued)

Field	Description
Total Recursive Paths	Number of buckets for recursive loadinfo. This is the number of paths available for a prefix learnt through BGP, or static recursive routes.
TLU1	Recursive loadinfo parameters.
SW/HW	HW: Information programmed in hardware. SW: Software shadow information.
local	Entry used to forward this traffic type only (if this bit is set). Note that this bit is used only for VPLS broadcast and multicast traffic forwarding.
next ptr	Next memory location for hardware lookup.
num of entries	Number of buckets for non-recursive loadinfo. This is the number of paths learned through IGP or static non-recursive routers.

Related Commands

Command	Description
show cef ipv6 external hardware	To display information related to IPv6 CEF external clients.

show cef ipv4 hardware

To display IPv4 CEF hardware status and configuration information, use the **show cef ipv4 hardware** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 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.
egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

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

```
RP/0/RP0/CPU0:router# show cef ipv4 hardware egress

Prefix              Next Hop            Interface
0.0.0.0/0           172.29.52.1         <recursive>
0.0.0.0/32          broadcast
10.1.1.1/32         receive             Loopback0
10.2.2.2/32         10.12.24.2          Bundle-POS24
10.6.6.6/32         10.16.8.6           GigabitEthernet0/6/5/2
10.7.7.7/32         10.12.24.2          Bundle-POS24
10.11.11.11/32      10.12.8.2           POS0/1/0/1
10.12.4.0/24        attached            POS0/6/4/5
10.12.4.0/32        broadcast           POS0/6/4/5
10.12.4.1/32        receive             POS0/6/4/5
10.12.4.255/32      broadcast           POS0/6/4/5
10.12.8.0/24        attached            POS0/1/0/1
10.12.8.0/32        broadcast           POS0/1/0/1
10.12.8.1/32        receive             POS0/1/0/1
10.12.8.255/32      broadcast           POS0/1/0/1
10.12.12.0/24       attached            POS0/6/0/1
```

Table 17 describes the significant fields shown in the display.

Table 17 show cef ipv4 hardware egress Field Descriptions

Field	Description
Prefix	Nonrecursive prefixes detected on the node.
Next Hop	Routing next hop.
Interface	Interface associated with the nonrecursive prefix.

Related Commands

Command	Description
show cef ipv6 hardware	Displays CEF IPv6 hardware status and configuration information.

show cef ipv4 interface

To display IPv4 Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef ipv4 interface** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 interface** *type instance* [**detail**] [**rpf-statistics**] [**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.
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 (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.
detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
rpf-statistics	(Optional) Displays the unicast reverse path forwarding (RPF) statistics.
location *node-id*	(Optional) Displays IPv4 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4 interface MgmtEth 0/RP0/CPU0/0

MgmtEth0/0/CPU0/0 is up (if_handle 0x01000100)
  Forwarding is enabled
  ICMP redirects are never sent
  IP MTU 1500, TableId 0xe0000000
  Reference count 2
```

Table 18 describes the significant fields shown in the display.

Table 18 show cef ipv4 interface Field Descriptions

Field	Description
MgmtEth 0/RP0/CPU0/0 is up	Status of the interface.
if_handle	Internal interface handle.
Forwarding is enabled	Indicates that CEF is enabled.
ICMP redirects are always sent or never sent	Indicates whether ICMP[1] redirect messages should be sent. By default, ICMP redirect messages are always sent.
IP MTU	Value of the IPv4 MTU[2] size set on the interface.
Reference count	Internal reference counter.

1. ICMP = internet control message protocol
2. MTU = maximum transmission unit

Related Commands

Command	Description
show cef ipv6 interface	Displays IPv6 CEF-related information for an interface.

show cef ipv4 interface bgp-policy-statistics

To display IPv4 Cisco Express Forwarding (CEF)-related BGP policy statistics information for an interface, use the **show cef ipv4 interface bgp-policy-statistics** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 interface** *type instance* **bgp-policy-statistics**

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.
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 (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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.0	This command was introduced on the Cisco CRS-1.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command displays all the configured BGP policy counters for the specified interface.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 interface bgp-policy-statistics** command:

```
RP/0/RP0/CPU0:router# show cef ipv4 interface TenGigE 0/2/0/4 bgp-policy-statistics

TenGigE0/2/0/4 is up
Input BGP policy accounting on src IP address enabled
buckets packets  bytes
0       184054   10157753
6       65688590 4204069760
7       65688590 4204069760
8       65688654 4204073856
9       65688656 4204073984
10      65688655 4204073920
30      32844290 1510837340
31      32844291 1510837386
32      32844294 1510837524
33      32844296 1510837616
34      32844298 1510837708
35      32844302 1510837892
36      32844302 1510837892
37      32844303 1510837938
38      32844305 1510838030
39      32844307 1510838122
Output BGP policy accounting on dst IP address enabled
buckets packets bytes
0       754     43878
Output BGP policy accounting on src IP address enabled
buckets packets bytes
0       857     51706
```

Table 19 describes the significant fields shown in the display.

Table 19 show cef ipv4 interface bgp-policy-statistics Field Descriptions

Field	Description
TenGigE 0/2/0/4 is up	Status of the interface.
Input BGP policy accounting on src IP address enabled	Enabled BGP policy accounting features.
buckets	Traffic index.
packets	Number of packets counted in the bucket.
bytes	Number of bytes counted in the bucket.

Related Commands

Command	Description
show cef ipv6 interface bgp-policy-statistics	Displays IPv6 CEF-related BGP policy statistics information for an interface.

show cef ipv4 non-recursive

To display the IPv4 nonrecursive prefix entries in the IPv4 CEF table, use the **show cef ipv4 non-recursive** command in 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 packet switch exchange (PSE).
ingress	(Optional) Displays ingress packet switch exchange (PSE).
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 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.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4 non-recursive

Prefix              Next Hop            Interface
0.0.0.0/0           12.8.0.1
0.0.0.0/32          broadcast
12.8.0.0/16         attached            MgmtEth0/0/CPU0/0
12.8.0.0/32         broadcast           MgmtEth0/0/CPU0/0
12.8.0.1/32         12.8.0.1            MgmtEth0/0/CPU0/0
12.8.0.2/32         12.8.0.2            MgmtEth0/0/CPU0/0
12.8.0.3/32         12.8.0.3            MgmtEth0/0/CPU0/0
12.8.16.10/32       12.8.16.10          MgmtEth0/0/CPU0/0
12.8.16.30/32       12.8.16.30          MgmtEth0/0/CPU0/0
12.8.16.40/32       12.8.16.40          MgmtEth0/0/CPU0/0
12.8.28.8/32        12.8.28.8           MgmtEth0/0/CPU0/0
12.8.28.101/32      12.8.28.101         MgmtEth0/0/CPU0/0
12.8.28.103/32      12.8.28.103         MgmtEth0/0/CPU0/0
12.8.28.104/32      12.8.28.104         MgmtEth0/0/CPU0/0
12.8.28.106/32      receive             MgmtEth0/0/CPU0/0
12.8.29.113/32      12.8.29.113         MgmtEth0/0/CPU0/0
12.8.29.118/32      12.8.29.118         MgmtEth0/0/CPU0/0
12.8.29.140/32      12.8.29.140         MgmtEth0/0/CPU0/0
12.8.33.101/32      12.8.33.101         MgmtEth0/0/CPU0/0
12.8.33.103/32      12.8.33.103         MgmtEth0/0/CPU0/0
12.8.33.105/32      12.8.33.105         MgmtEth0/0/CPU0/0
12.8.33.110/32      12.8.33.110         MgmtEth0/0/CPU0/0
12.8.57.1/32        12.8.57.1           MgmtEth0/0/CPU0/0
12.8.255.255/32     broadcast           MgmtEth0/0/CPU0/0
12.29.31.2/32       12.29.31.2          MgmtEth0/0/CPU0/0
223.255.0.0/16      attached            MgmtEth0/0/CPU0/0
223.255.254.254/32  223.255.254.254     MgmtEth0/0/CPU0/0
224.0.0.0/4         0.0.0.0
224.0.0.0/24        receive
```

Table 20 describes the significant fields shown in the display.

Table 20 show cef ipv4 non-recursive Field Descriptions

Field	Description
Prefix	Nonrecursive prefixes detected on the node.
Next Hop	Routing next hop.
Interface	Interface associated with the nonrecursive prefix.

Related Commands

Command	Description
show cef ipv6 non-recursive	Displays IPv6 nonrecursive prefix entries in the CEF table.

show cef ipv4 resources

To display IPv4 CEF resource availability status, use the **show cef ipv4 resources** command in EXEC mode.

show cef ipv4 resources [**detail**] [**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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4 resource detail

CEF resource availability summary state: GREEN
  ipv4 shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1874526208 bytes, MaxAvail 1875693568 bytes
  ipv6 shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1874591744 bytes, MaxAvail 1875365888 bytes
  mpls shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1874407424 bytes, MaxAvail 1875038208 bytes
  common shared memory resource:
        CurrMode GREEN, CurrUtil 0%
        CurrAvail 1873215488 bytes, MaxAvail 1874972672 bytes
  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
```

Table 21 describes the significant fields shown in the display.

Table 21 show cef ipv4 non-recursive Field Descriptions

Field	Description
Prefix	Nonrecursive prefixes detected on the node.
Next Hop	Routing next hop.
Interface	Interface associated with the nonrecursive prefix.

Related Commands

Command	Description
show cef ipv6 resources	Displays IPv6 CEF resource availability status.

show cef ipv4 summary

To display a summary of the IPv4 CEF table, use the **show cef ipv4 summary** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output from the **show cef ipv4 summary** command:

```
RP/0/RP0/CPU0:router# show cef ipv4 summary

Router ID is 0.0.0.0

IP CEF with switching (Table Version 43)
  tableid 0xe0000000, vrfid 0x60000000, vrfname unknown, vrid 0x20000000, flags
0x1
  34 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  0 load sharing elements, 0 bytes, 0 references
  0 CEF route update drops, 9 revisions of existing leaves
  Resolution Timer: 15s
  9 prefixes modified in place

Adjacency Table has 26 adjacencies
  2 incomplete adjacencies
```

Table 22 describes the significant fields shown in the display.

Table 22 show cef ipv4 summary Field Descriptions

Field	Description
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.

Related Commands

Command	Description
show cef ipv6 summary	Displays a summary of the IPv6 CEF table.

show cef ipv4 unresolved

To display unresolved routes in the IPv4 CEF table, use the **show cef ipv4 unresolved** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv4 unresolved** [**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 the unresolved routes in the IPv4 CEF table for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv4 unresolved

Prefix              Next Hop            Interface
3.3.3.3             2.2.2.2               ?
```

Table 23 describes the significant fields shown in the display.

Table 23 show cef ipv4 unresolved 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.

Related Commands

Command	Description
show cef ipv6 unresolved	Displays unresolved routes in the IPv6 CEF table.

show cef ipv6

To display the IPv6 Cisco Express Forwarding (CEF) table, use the **show cef ipv6** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	The sample output for the **detail** keyword is modified for a specific prefix.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv6

::/0

::/128
  drop
::1/128
  loopback
66::4/128
  receive    Loopback0
2222::/64
  connected  POS0/4/0/0
2222::1/128
  receive    POS0/4/0/0
3333::/64
  connected  POS0/3/0/0
3333::2/128
  receive    POS0/3/0/0
5656::2/128
  recursive  fe80::3031:48ff:fe53:5533, POS0/3/0/0
7777::/64
  connected  POS0/0/0/0
7777::2/128
  receive    POS0/0/0/0
9999::1/128
  recursive  fe80::205:5fff:fe1d:7600, POS0/4/0/0
ff00::/8
  drop
ff02::1/128
  receive
ff02::2/128
  receive
ff02::5/128
  receive
ff02::6/128
  receive
ff02::1:ff00:0/104
  receive
```

Table 24 describes the significant fields shown in the display.

Table 24 show cef ipv6 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:

```
RP/0/RP0/CPU0:router# show cef ipv6 detail
```

```
::/0
  flags: source_rib
  Loadinfo owner: <this route>
  fast adj: glean
  path 1:
    flags     :
    next hop  : ::
    interface : POS0/0/0/0

::/128
  flags: drop, source_fib
  Loadinfo owner: <this route>
  fast adj: drop
  path 1:
    flags     :
    next hop  : ::
    interface : <not specified>

::1/128
  flags: loopback, source_fib
  Loadinfo owner: <this route>
  fast adj: loopback
  path 1:
    flags     :
    next hop  : ::
    interface : <not specified>

66::4/128
  flags: receive, source_rib
  Loadinfo owner: <this route>
  fast adj: receive
  path 1:
    flags     : point-to-point
    next hop  : ::
    interface : Loopback0
```

Table 25 describes the significant output fields shown in the display.

Table 25 show cef ipv6 detail 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.

The following sample output is from the **show cef ipv6** command for the **detail** keyword, with 101:1:1::/64 as the *ipv6-prefix/prefix-length* argument and a location of 0/1/CPU0:

```
RP/0/RP0/CPU0:router# show cef ipv6 101:1:1::/64 detail location 0/1/CPU0

101:1:1::/64, version 262, internal 0x42000001[1]
 Prefix Len 64, traffic index 0, precedence routine (0)
  gateway array reference count 1, flags 0x0, [0, flags 0x4900]
  Level 1 - Load distribution: 0
  [0] via 22:6:1::9, recursive

   via 22:6:1::9, 0 dependencies, recursive
    next hop 22:6:1::9 via 22:6:1::9/128

    Load distribution: _ _ _ (refcount 1)

    Hash  OK  Interface                 Address
    -     Y   GigabitEthernet0/1/2/1    fe80::250:e2ff:fe8f:8381
    -     Y   POS0/1/0/2                ::
    -     Y   GigabitEthernet0/1/2/2    fe80::250:e2ff:fe8f:8382
```

Related Commands

Command	Description
show cef ipv4	Displays the IPv4 CEF table.

show cef ipv6 adjacency

To display IPv6 CEF adjacency status and configuration information, use the **show cef ipv6 adjacency** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 adjacency** [*interface-type interface-instance*] [**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-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 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.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 cef ipv6 adjacency** command:

```
RP/0/RP1/CPU0:ios# show cef ipv6 adjacency MgmtEth 0/RP1/CPU0/0


Display protocol is ipv6
Interface    Address                                          Type    Refcount

Mg0/RP1/CPU0/0Prefix: 12.25.0.3/32                             local   2
              Adjacency: PT:0x782a2900 12.25.0.3/32
              Interface: Mg0/RP1/CPU0/0
              MAC: 00.d0.02.75.ab.fd.00.11.93.ef.e3.50.08.00
              Interface Type: 0x8, Base Flags: 0x1
              Dependent adj type: remote
              Dependent adj intf: Mg0/RP1/CPU0/0

Mg0/RP1/CPU0/0Prefix: 0.24.0.32/32                             remote  6
              Adjacency: PT:0x782a2b58
              Interface: Mg0/RP1/CPU0/0
              MAC: 28.4e.4f.4e.45.29
              Interface Type: 0x8, Base Flags: 0x0
```

Table 26 describes the significant fields shown in the display.

Table 26 show cef ipv6 adjacency 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.

Related Commands

Command	Description
show cef ipv4 adjacency	Displays CEF IPv4 adjacency status and configuration information.

show cef ipv6 adjacency hardware

To displayIPv6 CEF adjacency hardware status and configuration information, use the **show cef ipv6 adjacency hardware** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 adjacency hardware** {**egress** | **ingress** [**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 packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 adjacency hardware** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 adjacency hardware

Interface    Address                                          Type    Refcount

Mg0/RP0/CPU0/0                                                 special 4
             Interface: Mg0/RP0/CPU0/0 Type:  glean
             Interface Type: 0x8, Base Flags: 0x4400
             Dependent adj type: remote
             Dependent adj intf: Mg0/RP0/CPU0/0

Mg0/RP0/CPU0/0Prefix: 64.102.12.47/32                          local   3
             Adjacency: PT:0x78f5c708 64.102.12.47/32
             Interface: Mg0/RP0/CPU0/0
             MAC: 00.30.f2.f2.10.38.00.11.93.ef.e8.e6.08.00
             Interface Type: 0x8, Base Flags: 0x1
             Dependent adj type: remote
             Dependent adj intf: Mg0/RP0/CPU0/0
```

Table 27 describes the significant fields shown in the display.

Table 27 show cef ipv6 adjacency hardware 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.

Related Commands

Command	Description
show cef ipv4 adjacency hardware	Displays CEF IPv4 adjacency hardware status and configuration information

show cef ipv6 drops

To display IPv6 CEF table packet drop counters, use the **show cef ipv6 drops** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv6 drops location 0/2/CPU0

 IPv6 CEF Drop Statistics
  Line status down      ingress :               0 egress :  Not Applicable
  Packet sanity fail    ingress :               0 egress :                0
  PLU set to drop       ingress :               0 egress :                0
  Unknown type,plu drop ingress :               0 egress :                0
  Packet length err     ingress :               0 egress :                0
  TCAM src-comp err     ingress :               0 egress :                0
```

Table 28 describes the significant fields shown in the display.

Table 28 show cef ipv6 drop Field Descriptions

Field	Description
Line status down	Packet drops due to the line protocol of the incoming interface being down.
Packet sanity fail	Packet drops due to the prefix failing the IPv6 sanity test. The sanity test verifies that the IPv6 packet is valid.
PLU set to drop	Packet drops due the IPv6 destination prefix being set to drop.
Unknown type, plu drop	Packet drops due to the prefix being of an unknown type.
Packet length errs	Length specified in the header does not match the actual length of the packet received.
TCAM src-comp err	Packet drops due to source compression errors that have occurred in the hardware.

Related Commands

Command	Description
clear cef ipv6 drops	Clears IPv6 CEF packet drop counters.

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 EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 exact-route** {*source-address destination-address*} [**detail** | **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 CEF entry 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 exact-route** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 exact-route 222::2 9999::6751 location

0/3/CPU0 source address: 222::2 destination address: 9999::6751
interface : TenGigE0/3/0/3 non local interface
```

Note In the example above, the show output does not require an explanation of the various fields.

Related Commands

Command	Description
show cef ipv4 exact-route	Displays the path an IPv4 flow comprising a source and destination address will take.

show cef ipv6 exceptions

To display IPv6 CEF exception packet counters, use the **show cef ipv6 exceptions** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router: show cef ipv6 exceptions location 0/3/CPU0

IPv6 CEF Exception Statistics
Node: 0/3/CPU0
  TTL err               ingress :               0 egress :  Not Applicable
  Link-local dst addr   ingress :               0 egress :               0
  Hop-by-Hop header     ingress :               0 egress :               0
  PLU entry set to punt ingress :               0 egress :               0
  Packet too big        ingress :  Not Applicable egress :               0
  Med priority punt     ingress :               0 egress :  Not Applicable
```

Table 29 describes the significant fields shown in the display.

Table 29 show cef ipv6 exceptions Field Descriptions

Field	Description
TTL err	Packets sent to software for processing because the packet header of the IPv6 prefix had a TTL[1] error.
Link-local dst addr	Packets sent to the software for processing because the destination address of the IPv6 prefix is link local.
Hop-by-Hop header	Packets sent to the software for processing because the IPv6 packet has a hop-by-hop header.
PLU entry set to punt	Packets sent to software for processing because the IPv6 prefix is set to punt.
Packet too big	Packets sent to the software for processing because the packet size exceeded the MTU[2].
Med priority punt	Field used internally for troubleshooting.

1. TTL = time to live
2. MTU = maximum transmission unit

Related Commands

Command	Description
clear cef ipv4 exceptions	Clears IPv4 CEF exception packet counters.

show cef ipv6 external hardware

To display CEF information related to CEF external clients, use the **show cef ipv6 external hardware** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 external hardare** {**ingress** | **detail**} **location** *node-id*]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
ingress	Display information read from the ingress packet switch exchange (PSE).
detail	Displays full information about CEF external clients.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show cef ipv6 external hardware** command displays every prefix that an external client is interested in as well as the hardware information from the platform.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output for the **show cef ipv6 external hardare** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 vrf_1 external hardare ingress location 0/1/0

Client Name       : l2fib_mgr
Interest type     : EOS0 LDI updates
Prefix            : 3.3.3.3/32
Number of notifs  : 1
State             : resolved, mismatch, cached plat context, in retry
Via               : drop

    Load distribution: 0 (refcount 0)

    Hash  OK  Interface                 Address
    0     Y   Unknown                   drop

    INGRESS External CLient Load info:
Total Recursive Paths 0
    TLU1 0x00004610 nexthop: 0.0.0.0
    TLU1 ENTRY        0
     SW: 0x00000002 00010000 00000000 00000100
     HW: 0x00000002 00010000 00000000 00000100
    local:                0x0    drop:               0x1
    next ptr:     0x00010000
    num of entries:    1
    Recursive next-hop:   0.0.0.0
```

Table 30 describes the significant fields shown in the display.

Table 30 show cef ipv4 external hardware Field Descriptions

Field	Description
Client Name	Process name of the client (for example, l2fib_mgr).
Interest type	Client interest type, which may be: • IP reachability notify • EOS0 LDI updates • IP LDI updates • 6VPE MPLS nexthop reachability • 6VPE IP tunnel nexthop reachability
Prefix	Client prefix. If the interest type is 6VPE, you will see Tunnel Id for the outgoing tunnel if the prefix length is not 0.
Number of notifs	Number of times the client has been notified about this prefix.
State	Client state, which may be: • resolved/unresolved • mismatch • path • notif pending • cached plat context • in retry • stale
Via	Next hop for this prefix.

Table 30 show cef ipv4 external hardware Field Descriptions (continued)

Field	Description
Total Recursive Paths	Number of buckets for recursive loadinfo. This is the number of paths available for a prefix learnt through BGP, or static recursive routes.
TLU1	Recursive loadinfo parameters.
SW/HW	HW: Information programmed in hardware. SW: Software shadow information.
next ptr	Next memory location for hardware lookup.
num of entries	Number of buckets for non-recursive loadinfo. This is the number of paths learned through IGP or static non-recursive routers.

Related Commands

Command	Description
show cef ipv4 external hardware	To display information related to IPv4 CEF external clients.

show cef ipv6 hardware

To display IPv6 CEF hardware status and configuration information, use the **show cef ipv6 hardware** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 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.
egress	Displays information from the egress packet switch exchange (PSE) file.
ingress	Displays information from the ingress packet switch exchange (PSE) file.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv6 hardware egress** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 hardware egress

Prefix               Next Hop            Interface
0.0.0.0/0            172.29.52.1         <recursive>
0.0.0.0/32           broadcast
10.1.1.1/32          receive             Loopback0
10.2.2.2/32          10.12.24.2          Bundle-POS24
10.6.6.6/32          10.16.8.6           GigabitEthernet0/6/5/2
10.7.7.7/32          10.12.24.2          Bundle-POS24
10.11.11.11/32       10.12.8.2           POS0/1/0/1
10.12.4.0/24         attached            POS0/6/4/5
10.12.4.0/32         broadcast           POS0/6/4/5
10.12.4.1/32         receive             POS0/6/4/5
10.12.4.255/32       broadcast           POS0/6/4/5
10.12.8.0/24         attached            POS0/1/0/1
10.12.8.0/32         broadcast           POS0/1/0/1
10.12.8.1/32         receive             POS0/1/0/1
10.12.8.255/32       broadcast           POS0/1/0/1
10.12.12.0/24        attached            POS0/6/0/1
```

Table 31 describes the significant fields shown in the display.

Table 31 show cef ipv6 hardware egress Field Descriptions

Field	Description
Prefix	Nonrecursive prefixes detected on the node.
Next Hop	Routing next hop.
Interface	Interface associated with the nonrecursive prefix.

Related Commands

Command	Description
show cef ipv4 hardware	Displays CEF IPv4 hardware status and configuration information.

show cef ipv6 interface bgp-policy-statistics

To display IPv6 Cisco Express Forwarding (CEF)-related BGP policy statistics information for an interface, use the **show cef ipv6 interface bgp-policy-statistics** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 interface** *type instance* **bgp-policy-statistics**

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.
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 (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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show cef ipv6 interface bgp-policy-statistics** command displays all the configured BGP policy counters for the specified interface.

Task ID

Task ID	Operations
cef	read

Examples

The following is sample output from the **show cef ipv4 interface bgp-policy-statistics** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 interface TenGigE 0/2/0/4 bgp-policy-statistics

TenGigE0/2/0/4 is up
Input BGP policy accounting on src IP address enabled
buckets packets  bytes
0       184054   10157753
6       65688590 4204069760
7       65688590 4204069760
8       65688654 4204073856
9       65688656 4204073984
10      65688655 4204073920
30      32844290 1510837340
31      32844291 1510837386
32      32844294 1510837524
33      32844296 1510837616
34      32844298 1510837708
35      32844302 1510837892
36      32844302 1510837892
37      32844303 1510837938
38      32844305 1510838030
39      32844307 1510838122
Output BGP policy accounting on dst IP address enabled
buckets packets bytes
0       754     43878
Output BGP policy accounting on src IP address enabled
buckets packets bytes
0       857     51706
```

Table 32 describes the significant fields shown in the display.

Table 32 show cef ipv6 interface bgp-policy-statistics Field Descriptions

Field	Description
TenGigE 0/2/0/4 is up	Status of the interface.
Input BGP policy accounting on src IP address enabled	Enabled BGP policy accounting features.
buckets	Traffic index.
packets	Number of packets counted in the bucket.
bytes	Number of bytes counted in the bucket.

Related Commands

Command	Description
show cef ipv4 interface bgp-policy-statistics	Displays IPv4 CEF-related BGP policy statistics information for an interface.

show cef ipv6 interface

To display IPv6 Cisco Express Forwarding (CEF)-related information for an interface, use the **show cef ipv6 interface** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 interface** *type instance* [**detail**] [**rpf-statistics**] [**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.
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 (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.
detail	(Optional) Displays detailed CEF information for all the interfaces on the node in which the command is issued.
rpf-statistics	(Optional) Displays the unicast reverse path forwarding (RPF) statistics.
location *node-id*	(Optional) Displays IPv6 CEF-related information for an interface. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output from the **show cef ipv6 interface** command:

```
RP/0/RP0/CPU0:router# show cef ipv6 interface MgmtEth 0/RP0/CPU0/0

MgmtEth0/0/CPU0/0 is up (if_handle 0x01000100)
  Forwarding is enabled
  ICMP redirects are never sent
  IP MTU 1500, TableId 0xe0000000
  Reference count 2
```

Table 33 describes the significant fields shown in the display.

Table 33 show cef ipv6 interface Field Descriptions

Field	Description
MgmtEth 0/RP0/CPU0/0 is up	Status of the interface.
if_handle	Internal interface handle.
Forwarding is enabled	Indicates that CEF is enabled.
ICMP redirects are always sent or never sent	Indicates whether ICMP[1] redirect messages should be sent. By default, ICMP redirect messages are always sent.
IP MTU	Value of the IPv4 MTU[2] size set on the interface.
Reference count	Internal reference counter.

1. ICMP = internet control message protocol
2. MTU = maximum transmission unit

Related Commands

Command	Description
show cef ipv4 interface	Displays IPv4 CEF-related information for an interface.

show cef ipv6 non-recursive

To display the nonrecursive prefix entries in the IPv6 CEF table, use the **show cef ipv6 non-recursive** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 non-recursive** [**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 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv6 non-recursive

::/0

::/128
  drop
::1/128
  loopback
66::4/128
  receive    Loopback0
2222::/64
  connected  POS0/4/0/0
2222::1/128
  receive    POS0/4/0/0
3333::/64
  connected  POS0/3/0/0
3333::2/128
  receive    POS0/3/0/0
7777::/64
  connected  POS0/0/0/0
7777::2/128
  receive    POS0/0/0/0
ff00::/8
  drop
ff02::1/128
  receive
ff02::2/128
  receive
ff02::5/128
  receive
ff02::6/128
  receive
ff02::1:ff00:0/104
  receive
```

Table 34 describes the significant fields shown in the display.

Table 34 show cef ipv6 non-recursive 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.

Related Commands

Command	Description
show cef ipv4 non-recursive	Displays IPv4 nonrecursive prefix entries in the CEF table.

show cef ipv6 resources

To display IPv6 CEF resource availability status, use the **show cef ipv6 resources** command in EXEC mode.

show cef ipv6 resources [**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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0: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
```

Note In the example above, the show output does not require an explanation of the various fields.

Related Commands

Command	Description
show cef ipv4 resources	Displays IPv4 CEF resource availability status.

show cef ipv6 summary

To display a summary of the IPv6 CEF table, use the **show cef ipv6 summary** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv6 summary

IPv6 CEF with switching (Table Version 0)
  9 routes, 0 background, 0 pending, 0 unresolved paths
  9 load sharing elements, 324 bytes, 9 references
  3384 bytes fib leaf memory

Router ID is 0.0.0.0
Adjacency Table has 15 adjacencies
  2 incomplete adjacencies
```

Table 35 describes the significant fields shown in the display.

Table 35 show cef ipv6 summary Field Descriptions

Field	Description
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.

Related Commands

Command	Description
show cef ipv4 summary	Displays a summary of the IPv4 CEF table.

show cef ipv6 unresolved

To display the unresolved routes in the IPv6 CEF table, use the **show cef ipv6 unresolved** command in EXEC mode.

show cef [**vrf** *vrf-name*] **ipv6 unresolved** [**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 the unresolved routes in the IPv6 CEF table for the specified node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show cef ipv6 unresolved

9999::/64
  unresolved
```

Table 36 describes the significant fields shown in the display.

Table 36 show cef ipv6 unresolved Field Descriptions

Field	Description
xxxx::/*xx*	Detected unresolved route.

Related Commands

Command	Description
show cef ipv4 unresolved	Displays unresolved routes in the IPv4 CEF table.

show cef mpls adjacency

To display the Multiprotocol Label Switching (MPLS) adjacency table, use the **show cef mpls adjacency** command in EXEC mode.

show cef mpls adjacency [*interface-type interface-instance*] [**location** *node-id*]

Syntax Description

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 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.
location *node-id*	(Optional) Displays detailed CEF information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 mpls adjacency** command:

```
RP/0/RP0/CPU0:router# show cef mpls adjacency

Display protocol is mpls
Interface    Address                                          Type    Refcount

BP24         Prefix: 0/0                                      local   10
             no next-hop adj
             Interface: None
             Mac-length is 0
             incomplete
             Interface Type: 0x1d, Base Flags: 0x100
             Dependent adj type: remote
             Dependent adj intf: BP24
```

Related Commands

Command	Description
show cef mpls unresolved	Displays Multiprotocol Label Switching (MPLS) unresolved routes.

show cef mpls unresolved

To display the Multiprotocol Label Switching (MPLS) unresolved routes, use the **show cef mpls unresolved** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef mpls unresolved** command:

```
RP/0/RP0/CPU0:router# show cef mpls unresolved

Label/EOS           Next Hop            Interface
```

Related Commands

Command	Description
show cef mpls adjacency	Displays the Multiprotocol Label Switching (MPLS) adjacency table.

show cef vrf

To display the contents of the VPN routing and forwarding (VRF) instance, use the **show cef vrf** command in EXEC mode.

show cef vrf [*vrf-name*]

Syntax Description

vrf-name	Name of the VRF instance.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
cef	read

Examples

This following is sample output from **show cef vrf** command when an unresolved route is detected:

```
RP/0/RP0/CPU0:router# show cef vrf 0

Prefix              Next Hop            Interface
0.0.0.0/0           drop                default handler
0.0.0.0/32          broadcast
224.0.0.0/24        receive
255.255.255.255/32  broadcast
```

Table 37 describes the significant fields shown in the display.

Table 37 show cef vrf Field Descriptions

Field	Description
Prefix	Prefix in the IPv4 CEF table.
Next Hop	Next hop of the prefix.
Interface	Interface associated with the prefix.

DHCP Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure and monitor the Dynamic Host Configuration Protocol (DHCP).

allow-hint

To allow the server to delegate a valid client-suggested prefix in the solicit and request messages, use the **allow-hint** command in DHCP IPv6 interface server configuration mode. To disable the delegation of a valid client-suggested prefix, use the **no** form of the command.

allow-hint

no allow-hint

Syntax Description

This command has no arguments or keywords.

Defaults

DHCPv6 service on an interface is disabled.

Command Modes

DHCP IPv6 interface server configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **allow-hint** command enables the server to delegate a client-suggested prefix in the solicit and request messages if the prefix in the associated local prefix pool is a valid prefix and it is not assigned to any other solicit and request messages. Otherwise, the hint is ignored, and a prefix is delegated from the free list in the pool.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of the **allow-hint** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dhcp ipv6 interface pos 0/5/0/0 server
RP/0/RP0/CPU0:router(config-dhcpv6-if)# allow-hint
```

clear dhcp ipv6 binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding table, use the **clear ipv6 dhcp binding** command in EXEC mode.

clear dhcp ipv6 binding [*ipv6-address*]

Syntax Description

ipv6-address	(Optional) Address of a DHCP for an IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear ipv6 dhcp binding** command is used as a server function.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration information pool
- Updated when the client renews, rebinds, or confirms the prefix delegation
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the **clear ipv6 dhcp binding** command is used with the optional *ipv6-address* argument specified, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the *ipv6-address* argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table.

Task ID

Task ID	Operations
ip-services	execute

Examples

The following example specifies DHCP for IPv6 binding database agent parameters:

```
RP/0/RP0/CPU0:router# clear dhcp ipv6 binding
```

Related Commands

Command	Description
show dhcp ipv6 database	Displays the DHCP for the IPv6 binding database information.

database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **database** command in DHCP IPv6 configuration mode. To delete the database agent, use the **no** form of this command.

database *agent-URL* [**write-delay** *seconds*] [**timeout** *seconds*]

no database *agent-URL*

Syntax Description

agent-URL	A Flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
t**imeout** *seconds*	Optional) How long, in seconds, the router waits for a database transfer.

Defaults

Write-delay default is 300 seconds.
Timeout default is 300 seconds

Command Modes

DHCP IPv6 configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are aborted. By default, the DHCP for IPv6 server waits 300 seconds before aborting a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example specifies DHCP for IPv6 binding database agent parameters:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# database tftp://10.0.0.1/dhcp-binding
```

Related Commands

Command	Description
show dhcp ipv6 database	Displays the DHCP for the IPv6 binding database information.
interface (DHCP)	Enables DHCP for IPv6 on an interface

destination

To specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface, use the **destination** command in DHCP IPv6 interface relay configuration mode. To remove a relay destination on the interface or delete an output interface for a destination, use the **no** form of this command.

destination {*ipv6 address*} *interface*

no destination {*ipv6 address*} *interface*

Syntax Description

ipv6 address address	IPv6 address in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
interface	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.

Defaults

Relay function is disabled and there is no relay destination on the interface.

Command Modes

DHCP IPv6 interface relay configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **destination** command specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface is forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are the following two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface
- A global or site-scope unicast IPv6 address, for which a user can specify an output interface for this kind of address.
- A global or site-scope multicast IPv6 address, for which a user can specify an output interface for this kind of address if 'mhost ipv6 default-interface' is specified.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The **no** form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCP for IPv6 client, server, and relay functions is mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: “Interface is in DHCP client mode,” “Interface is in DHCP server mode,” or “Interface is in DHCP relay mode.”

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of the **destination** command on a Packet over Sonet/SDH (POS) interface:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 interface pos 0/5/0/0 relay
RP/0/RP0/CPU0:router(config-dhcpv6-if)# destination 10:10::10
```

Related Commands

Command	Description
interface (DHCP)	Enables DHCP for IPv6 on an interface.

distance

To specify an administrative distance for Dynamic Host Configuration Protocol (DHCP) for IPv6 Prefix Delegation, use the **distance** command in DHCP IPv6 configuration mode. To delete an administrative distance, use the **no** form of this command.

distance *administrative distanc*e

no distance *administrative distanc*e

Syntax Description

*administrative distanc*e	User defined distance. The range is 1 to 255.

Defaults

administrative distance: 1

Command Modes

DHCP IPv6

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of setting the DHCP administrative distance to 200 using the **distance** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router (config-dhcpv6)# distance 200
```

duid

To define the Dynamic Host Configuration Protocol (DHCP) the unique identification (DUID) on a specified device, use the **duid** command in DHCP IPv6 configuration mode. To delete an administrative distance, use the **no** form of this command.

duid *duid name*

no duid *duid name*

Syntax Description

duid name	IPv6 DHCP unique identifier (DUID) in hex format. The length of DUID word should be even.

Defaults

DUID-LL as defined in Section 9.4 of RFC3315

Command Modes

DHCP IPv6 configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **duid** command to configure the DHCP unique identifier on a specified device. Use the **no** form of this command to restore the default.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of how to create an IPv6 DHCP unique identifier (DUID) of 0002000000090CC084D303000912 using the **duid** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# duid 0002000000090CC084D303000912
```

Related Commands

Command	Description
show dhcp ipv6	Displays the DHCP DUID on a specified device.

dns-server

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Syntax Description

ipv6-address	IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

Defaults

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP IPv6 pool configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses do not overwrite old addresses.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of setting the DNS server name using the **dns-server** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)# dns-server 10:10::10
```

Related Commands

Command	Description
pool	Configures a DHCP for the IPv6 server configuration information pool and enters the IPv6 pool configuration mode.

domain-name

To configure a domain name for a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **domain-name** command in DHCP IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *domain*

no domain-name

Syntax Description

domain	Specifies the domain name string to be used by the client.

Defaults

When a DHCP for IPv6 pool is first created, no domain name for clients is configured.

Command Modes

DHCP IPv6 pool configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Multiple Domain Name System (DNS) domain names can be configured by issuing the **domain-name** command multiple times. The new domain name does not overwrite existing domain names.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of how to configure a DHCP IPv6 domain name using the **domain-name** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)# domain-name howie.com
```

Related Commands

Command	Description
pool	Configures a DHCP for the IPv6 server configuration information pool and enters the IPv6 pool configuration mode.

dhcp relay information check disable

To configure a Dynamic Host Configuration Protocol (DHCP) server to not validate the relay agent information option in forwarded BOOTREPLY messages, use the **dhcp relay information check disable** command in global configuration mode. To enable the information check and return to the default behavior, use the **no** form of this command.

dhcp relay information check disable

no dhcp relay information check disable

Syntax Description

This command has no arguments or keywords.

Defaults

DHCP validates the relay agent information option.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, DHCP validates the relay agent information option in forwarded BOOTREPLY messages. Use the **dhcp relay information check disable** command to disable the information check.

Task ID

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

Examples

The following example shows how to configure the relay agent to not validate the relay information option (Option 82) in a BOOTREPLY:

```
RP/0/RP0/CPU0:router(config)# dhcp relay information check disable
```

Related Commands

Command	Description
dhcp relay information option	Configures a DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).
dhcp server	Enables DHCP services on a networking device.

dhcp relay information option

To configure a Dynamic Host Configuration Protocol (DHCP) server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages, use the **dhcp relay information option** command in global configuration mode. To disable the insertion of relay information into forwarded BOOTREQUEST messages, use the **no** form of this command.

dhcp relay information option

no dhcp relay information option

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **dhcp relay information option** command to configure a DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages. Use the **no** form of this command to restore the default setting.

This command is used by cable access router termination systems. This functionality enables a DHCP server to identify the user (cable access router) sending the request and initiate appropriate action based on this information. By default, DHCP does not insert relay information.

Task ID

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

Examples

The following example shows how to enable command functionality and configure a DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages:

```
RP/0/RP0/CPU0:router(config)# dhcp relay information option
```

Related Commands

Command	Description
dhcp relay information check disable	Configures a DHCP server to not validate the relay agent information option in forwarded BOOTREPLY messages.
dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

dhcp relay information policy

To configure the information reforwarding policy for a Dynamic Host Configuration Protocol (DHCP) relay agent (what a relay agent should do if a message already contains relay information), use the **dhcp relay information policy** command in global configuration mode. To restore the default relay information policy, use the **no** form of this command.

dhcp relay information policy {**drop** | **keep** | **replace**}

no dhcp relay information policy {**drop** | **keep** | **replace**}

Syntax Description

drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
keep	Indicates that existing information is left unchanged on the DHCP relay agent.
replace	Indicates that existing information is overwritten on the DHCP relay agent.

Defaults

The DHCP server replaces existing relay information.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **dhcp relay information policy** command to configure the information reforwarding policy for a DHCP relay agent. Use the **no** form of this command to restore the default relay information policy.

This command is used by cable access router termination systems. When a DHCP relay agent receives a message from another DHCP relay agent, relay information might already be present in the message. By default, the relay information from the previous relay agent is replaced.

Task ID

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

Examples

The following examples show how to configure a DHCP relay agent to drop messages with existing relay information, keep existing information, and replace existing information, respectively:

```
RP/0/RP0/CPU0:router(config)# dhcp relay information policy drop
RP/0/RP0/CPU0:router(config)# dhcp relay information policy keep
RP/0/RP0/CPU0:router(config)# dhcp relay information policy replace
```

Related Commands

Command	Description
dhcp relay information check disable	Configures a DHCP server to not validate the relay agent information option in forwarded BOOTREPLY messages.
dhcp relay information option	Configures a DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.

dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) services on a networking device, use the **dhcp server** command in global configuration mode. To disable DHCP services, use the **no** form of this command.

dhcp server

no dhcp server

Syntax Description

This command has no arguments or keywords.

Defaults

DHCP services are disabled, which means the relay agent is off.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When this command is enabled, by default the relay agent is on.

Task ID

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

Examples

The following example shows how to enable DHCP services:

```
RP/0/RP0/CPU0:router(config)# dhcp server
```

Related Commands

Command	Description
dhcp relay information check disable	Configures a DHCP server to not validate the relay agent information option in forwarded BOOTREPLY messages.
dhcp relay information option	Configures a DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

interface (DHCP)

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 on an interface, use the **interface** command in DHCP IPv6 configuration mode. To disable DHCPv6 on an interface, use the **no** form of the command.

interface *interface-type interface-instance* {**server** | **relay**}

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 (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.
server	Enables service on the specified interface using the pool for prefix delegation.
relay	Specifies a destination address.

Defaults

No default behavior or values

Command Modes

DHCP IPv6 configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of enabling the DHCP interface mode on a Packet over Sonet/SDH (POS) interface using the **interface** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 interface POS 0/5/0/0 relay
```

Related Commands

Command	Description
show dhcp ipv6 interface	Displays DHCP for IPv6 interface information.

pd (prefix-delegation - DHCP IPv6 pool)

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **pd** command in DHCP IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

pd *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [**lifetime**]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. 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	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).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.
lifetime	(Optional) Sets a length of time during which the requesting router is allowed to use the prefix. The following values can be used: • valid-seconds—Length of time, in seconds, that the prefix remains valid for the requesting router to use. • valid-seconds preferred-seconds—Length of time, in seconds, that the prefix remains valid for the requesting router to use, plus the length of time after which client should re-check that it still has the prefix. • at—Absolute point in time where the prefix is no longer valid and no longer preferred. • preferred-seconds—Length of time, in seconds, that the prefix remains preferred for the requesting router to use. • infinite—Unlimited lifetime. This value can be used in place of valid-seconds or preferred-seconds value. • valid-month valid-date valid-year valid-time—Fixed duration of time for hosts to remember router advertisements. The format used can be oct 24 2003 11:45 or 24 oct 2003 11:45. • preferred-month preferred-date preferred-year preferred-time—Fixed duration of time for hosts to remember router advertisements. The format used can be oct 24 2003 11:45 or 24 oct 2003 11:45. • at valid-timestamp—Absolute point in time (rather than duration) for the valid-timestamp.The prefix is valid up to valid-timestamp. • at valid-timestamp preferred-timestamp—Absolute point in time (rather than duration) for the valid-timestamp and preferred time-stamp. The client should confirm that it has the prefix after preferred-timestamp; however, the time-stamp is still valid up to valid-timestamp.

Defaults

No manually configured prefix delegations exist.

Command Modes

DHCP IPv6 pool configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of the **pd** command in DHCP IPv6 pool configuration mode:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)# pd 2001:420:10::/48 0002000000090CC084D303000912
```

Related Commands

Command	Description
pool	Configures a DHCP for the IPv6 server configuration information pool and enters the IPv6 pool configuration mode.

pd (prefix-delegation - DHCP IPv6 interface)

To allow the identification of a client based on client connection to a specific interface, use the **pd** command in DHCP IPv6 interface server configuration mode. To remove the prefix, use the **no** form of this command.

pd *ipv6-prefix/prefix-length* [**lifetime**]

no pd *ipv6-prefix/prefix-length* [**lifetime**]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. 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	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).
lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • valid-lifetime—The length of time, in seconds, that the prefix remains valid for the requesting router to use. • at—Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • infinite—Indicates an unlimited lifetime. • preferred-lifetime—The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • valid-month valid-date valid-year valid-time—A fixed duration of time for hosts to remember router advertisements. The format used can be oct 24 2003 11:45 or 24 oct 2003 11:45. • preferred-month preferred-date preferred-year preferred-time—A fixed duration of time for hosts to remember router advertisements. The format used can be oct 24 2003 11:45 or 24 oct 2003 11:45.

Defaults

No manually configured prefix delegations exist.

Command Modes

DHCP IPv6 interface server configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of the **pd** command in DHCP IPv6 pool configuration mode:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)# exit
RP/0/RP0/CPU0:router(config-dhcpv6)# interface POS 0/5/0/0 server
RP/0/RP0/CPU0:router(config-dhcpv6-if)# pd 2001:420:10::/48
RP/0/RP0/CPU0:router(config-dhcpv6-if)# pool pool1
```

Related Commands

Command	Description
interface (DHCP)	Enables DHCP for IPv6 on an interface.

pool

To configure a Dynamic Host Configuration Protocol (DHCP) for the IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **pool** command in either DHCP IPv6 configuration mode or DHCP IPv6 interface relay configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

pool *poolname*

no pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as “Engineering”) or an integer (such as 0).

Defaults

No DHCP for IPv6 pools are configured.

Command Modes

DHCP IPv6 configuration

DHCP IPv6 interface server configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **pool** command to create a DHCP for IPv6 server configuration information pool. When the **pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers.

Once the DHCP for IPv6 configuration information pool has been created, use the **server** command to associate the pool with a server on an interface.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example show how to enter pool configuration mode using the **pool** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)#
```

Related Commands

Command	Description
show dhcp ipv6 pool	Displays DHCP for IPv6 configuration information pool information.

preference

To configure the preference value, use the **preference** command in DHCP IPv6 interface server configuration mode. To disable the preference value, use the **no** form of the command.

preference *preference value*

no preference

Syntax Description

preference value	Preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255.

Defaults

The preference value defaults to zero.

Command Modes

DHCP IPv6 interface server configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **preference** command configures a preference value. If the preference value is configured and it is not 0, the server adds a preference option to carry the preference value for the advertise message to a client to affect the selection of a server by client.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of the **preference** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# interface pos 0/5/0/0 server
RP/0/RP0/CPU0:router(config-dhcpv6-if)# preference 10
```

Related Commands

Command	Description
interface (DHCP)	Enables DHCP for IPv6 on an interface.

rapid-commit

To enable clients that specify the Rapid Commit option in their Solicit messages to receive immediate address assignment Reply messages, use the **rapid-commit** command in DHCP IPv6 interface server mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

rapid-commit

no rapid-commit

Syntax Description

This command has no arguments or keywords.

Defaults

Rapid commit is disabled.

Command Modes

DHCP IPv6 interface server configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **rapid-commit** command enables or disables rapid commit. If enabled, the DHCPv6 server uses the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and rapid-commit is enabled for the server, the server responds to the solicit message with a reply message. If rapid-commit is not enabled, then normal four-message exchange is done even if the clients specifies the rapid commit option.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following is an example of the **rapid-commit** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# interface pos 0/5/0/0 server
RP/0/RP0/CPU0:router(config-dhcpv6-if)# rapid-commit
```

Related Commands

Command	Description
interface (DHCP)	Enables DHCP for IPv6 on an interface.

show dhcp ipv6

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show dhcp ipv6** command in EXEC mode.

show dhcp ipv6

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv6** command:

```
RP/0/RP0/CPU0:router: show dhcp ipv6

This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

Related Commands

Command	Description
duid	Defines the DHCP unique identification (DUID) on a specified device.

show dhcp ipv6 binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in EXEC mode.

show dhcp ipv6 binding [*ipv6-address*]

Syntax Description

ipv6-address	(optional) IPv6 address. The *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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show dhcp ipv6 binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv6 binding** displaying all automatic client bindings from the DHCPv6 database. The *ipv6 address* argument is not specified:

```
RP/0/RP0/CPU0:router: show dhcp ipv6 binding

  Client: FE80::202:FCFF:FEA5:DC39 (Ethernet2/1)
    DUID: 000300010002FCA5DC1C
    IA PD: IA ID 0x00040001, T1 0, T2 0
      Prefix: 3FFE:C00:C18:11::/68
              preferred lifetime 180, valid lifetime 12345
              expires at Nov 08 2002 02:24 PM (12320 seconds)
  Client: FE80::202:FCFF:FEA5:C039 (Ethernet2/1)
```

```
DUID: 000300010002FCA5C01C
IA PD: IA ID 0x00040001, T1 0, T2 0
  Prefix: 3FFE:C00:C18:1::/72
          preferred lifetime 240, valid lifetime 54321
          expires at Nov 09 2002 02:02 AM (54246 seconds)
  Prefix: 3FFE:C00:C18:2::/72
          preferred lifetime 300, valid lifetime 54333
          expires at Nov 09 2002 02:03 AM (54258 seconds)
  Prefix: 3FFE:C00:C18:3::/72
          preferred lifetime 280, valid lifetime 51111
          expires at Nov 09 2002 01:09 AM (51036 seconds)
```

Table 38 describes the significant fields shown in the display.

Table 38 show dhcp ipv6 binding Command Field Descriptions

Field	Description
DUID	DHCP IPv6 unique identifier
IA PD	Identity Association for Prefix Delegation
Prefix	Prefixes delegated to the IAPD on the specified client

show dhcp ipv6 database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show dhcp ipv6 database** command in EXEC mode.

show dhcp ipv6 database [*agent-URL*]

Syntax Description

agent-URL	(Optional) Flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Each permanent storage to which the binding database is saved is called the *database agent*. An agent can be configured using the **dhcp ipv6 database** command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The **show dhcp ipv6 database** command displays DHCP for IPv6 binding database agent information. If the *agent-URL* argument is specified, only the specified agent is displayed. If the *agent-URL* argument is not specified, all database agents are shown.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv6 database** command:

```
RP/0/RP0/CPU0:router: show dhcp ipv6 database

  Database agent tftp://172.19.216.133/db.tftp:
    write delay: 69 seconds, transfer timeout: 300 seconds
    last written at Jan 09 2003 01:54 PM,
        write timer expires in 56 seconds
    last read at Jan 06 2003 05:41 PM
    successful read times 1
```

```
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
      write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
      write timer expires in 50 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2220
  failed write times 614
```

Table 39 describes the significant fields shown in the display.

Table 39 show dhcp ipv6 database Command Field Descriptions

Field	Description
Database agent	Specifies the database agent.
Write delay	The amount of time (in seconds) to wait before updating the database.
transfer timeout	Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted.
Last written	The last date and time bindings were written to the file server.
Write timer expires...	The length of time, in seconds, before the write timer expires
Last read	The last date and time bindings were read from the file server.
Successful/failed read times	The number of successful or failed read times.
Successful/failed write times	The number of successful or failed write times.

Related Commands

Command	Description
database	Configures a DHCP for IPv6 binding database agent.

show dhcp ipv6 interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show dhcp ipv6 interface** command in EXEC mode.

show dhcp ipv6 interface *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 (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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv6 interface** command when an interface is not specified:

```
RP/0/RP0/CPU0:router: show dhcp ipv6 interface

POS 0/5/0/0 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Hint from client: ignored
  Rapid-Commit: ignored
```

Table 40 describes the significant fields shown in the display.

Table 40 show dhcp ipv6 interface Command Field Descriptions

Field	Description
POS 0/5/0/0 is in server/relay mode	Displays whether the specified interface is in server or relay mode.
Using pool	Name of the pool used by the interface.
Preference value	Advertised (or default of 0) preference value for the indicated server.
Hint from client	Displays whether the allow-hint has been enabled on the interface.
Rapid-Commit	Displays whether the rapid-commit keyword has been enabled on the interface.

Related Commands

Command	Description
interface (DHCP)	Enables DHCP for IPv6 on an interface.

show dhcp ipv6 pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration information pool information, use the **show ipv6 dhcp pool** command in EXEC mode.

show dhcp ipv6 pool [*pool-name*]

Syntax Description

pool-name	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **dhcp ipv6 pool** command to create a configuration information pool, and use the **dhcp ipv6 server** command to associate the configuration information pool with a server on an interface.

The **show dhcp ipv6 pool** command displays DHCP for IPv6 configuration information pool information. If the *poolname* argument is specified, only information on the specified pool is displayed. If the *poolname* argument is not specified, all pools are shown.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show dhcp ipv6 pool** command. If *pool-name* is not specified, all pools are shown; otherwise, only the named pool is displayed.

```
RP/0/RP0/CPU0:router: show dhcp ipv6 pool

  DHCPv6 pool: svr-p1
    Static bindings:
      Binding for client 000300010002FCA5C01C
        IA PD: IA ID 00040002,
          Prefix: 3FFE:C00:C18:3::/72
                  preferred lifetime 604800, valid lifetime 2592000
```

```
     IA PD: IA ID not specified; being used by 00040001
       Prefix: 3FFE:C00:C18:1::/72
               preferred lifetime 240, valid lifetime 54321
       Prefix: 3FFE:C00:C18:2::/72
               preferred lifetime 300, valid lifetime 54333
       Prefix: 3FFE:C00:C18:3::/72
               preferred lifetime 280, valid lifetime 51111
 DNS server: 1001::1
 DNS server: 1001::2
 Domain name: domain1.net
 Domain name: domain2.net
 Domain name: domain3.net
Active clients: 2
```

Table 41 describes the significant fields shown in the display.

Table 41 show ipv6 dhcp pool Command Field Descriptions

Field	Description
DHCPv6 pool	The name of the pool.
IA PD	Identity association for prefix delegation (IA PD), which is a collection of prefixes assigned to a client.
Prefix	Prefixes to be delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	Lifetimes associated with the prefix statically assigned to the specified client.
DNS server	IPv6 addresses of the DNS servers.
Domain name	Displays the DNS domain search list.
Active clients	Total number of active clients.

show dhcp relay

To display Dynamic Host Configuration Protocol (DHCP) relay agent status, use the **show dhcp relay** command in EXEC mode.

show dhcp relay

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read

Examples

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

```
RP/0/RP0/CPU0:router: show dhcp relay
```

sip address

To configure a Session Initiation Protocol (SIP) server IPv6 address to be returned in the SIP server's IPv6 address list option to clients, use the **sip address** command in DHCP IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip address *ipv6 address*

no sip address *ipv6 address*

Syntax Description

ipv6-address	IPv6 address. The *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.

Defaults

No default behavior or values

Command Modes

DHCP IPv6 pool configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module of the *Cisco IOS XR System Security Command Reference*.

The **sip address** command configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients. To configure multiple SIP server addresses, issue this command multiple times. The new addresses do not overwrite old ones.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the SIP address using the **sip-address** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)# sip address 10:10::10
```

Related Commands

Command	Description
pool	Configures a DHCP for the IPv6 server configuration information pool and enters the IPv6 pool configuration mode.

sip domain-name

To configure a Session Initiation Protocol (SIP) server domain name to be returned in the SIP server's domain name list option to clients, use the **sip domain-name** command in DHCP IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip domain-name *domain-name*

no sip domain-name *domain-name*

Syntax Description

domain-name	A domain name for a DHCP for IPv6 client.

Defaults

No default behavior or values

Command Modes

DHCP IPv6 pool configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module of the *Cisco IOS XR System Security Command Reference*.

The **sip domain-name** command configures a SIP server domain name to be returned in the SIP server's domain name list option to clients. To configure multiple SIP server domain names, issue this command multiple times. The new domain names do not overwrite old ones.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the SIP address using the **sip domain-name** command:

```
RP/0/RP0/CPU0:router(config)# dhcp ipv6 pool pool1
RP/0/RP0/CPU0:router(config-dhcpv6-pool)# sip domain-name domain1.com
```

Related Commands

Command	Description
pool	Configures a DHCP for the IPv6 server configuration information pool and enters the IPv6 pool configuration mode.

Host Services and Applications Commands on Cisco IOS XR Software

This chapter describes the commands used to configure and monitor host services and applications, such as Domain Name System (DNS), Telnet, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), and rcp on Cisco IOS XR software.

For detailed information about host services and applications concepts, configuration tasks, and examples, see *Cisco IOS XR IP Addresses and Services Configuration Guide*.

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 global configuration 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.

Defaults

One service request per second is accepted.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# cinetd rate-limit 10
```

clear host

To delete temporary entries from the hostname-to-address cache, use the **clear host** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# clear host *
```

Related Commands

Command	Description
domain ipv4 host	Defines a static IPv4 hostname-to-address mapping in the host cache.
domain ipv6 host	Defines a static IPv6 hostname-to-address mapping in the host cache.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

domain ipv4 host

To define a static hostname-to-address mapping in the host cache using IPv4, use the **domain ipv4 host** command in global configuration 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 v4address1* [*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.

Defaults

No static mapping is configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router(config)# domain ipv4 host host1 192.168.7.18
RP/0/RP0/CPU0: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 global configuration 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.

Defaults

No static mapping is configured. IPv6 address prefixes are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router(config)# domain ipv6 host host1 ff02::2
RP/0/RP0/CPU0: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 global configuration 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.

Defaults

No domain names are defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If there is no domain list, the domain name that you specified with the **domain name** 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** 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:

```
RP/0/RP0/CPU0:router(config)# domain list domain1.com
RP/0/RP0/CPU0:router(config)# domain list domain2.edu
```

The following example shows how to add a name to and then delete a name from the list:

```
RP/0/RP0/CPU0:router(config)# domain list domain3.edu
RP/0/RP0/CPU0:router(config)# no domain list domain2.edu
```

Related Commands

Command	Description
domain name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

domain lookup disable

To disable the IP Domain Name System (DNS)-based hostname-to-address translation, use the **domain lookup disable** command in global configuration 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 arguments or keywords.

Defaults

The IP DNS-based host-to-address translation is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router(config)# domain lookup disable
```

Related Commands

Command	Description
domain name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
domain name-server	Specifies the address of one or more name servers to use for name and address resolution.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

domain name

To define a default domain name that the software uses to complete unqualified hostnames, use the **domain name** command in global configuration 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.

Defaults

There is no default domain name.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Examples

The following example shows how to define cisco.com as the default domain name:

```
RP/0/RP0/CPU0:router(config)# domain name cisco.com
```

Related Commands

Command	Description
domain list	Defines a list of default domain names to complete unqualified hostnames.
domain name-server	Specifies the address of one or more name servers to use for name and address resolution.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

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 global configuration 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.

Defaults

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

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.111
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.2
```

Related Commands

Command	Description
domain lookup disable	Disables the domain lookup.
domain name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).

ftp client anonymous-password

To assign a password for anonymous users, use the **ftp client anonymous-password** command in global configuration 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 Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **ftp client anonymous-password** command is 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:

```
RP/0/RP0/CPU0:router(config)# ftp client anonymous-password xxxx
```

ftp client passive

To configure the software to use only passive FTP connections, use the **ftp client passive** command in global configuration 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 arguments or keywords.

Defaults

FTP data connections are active.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0: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.
```

Related Commands

Command	Description
ftp client source-interface	Specifies the source IP address for FTP connections.

ftp client source-interface

To specify the source IP address for FTP connections, use the **ftp client source-interface** command in global configuration 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 instance*

no ftp client source-interface *type instance*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

The FTP source address is the IP address of the interface used by the FTP packets to leave the networking device.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 Packet-over-SONET (POS) interface 0/1/2/1 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
RP/0/RP0/CPU0:router(config)# ftp client source-interface POS 0/1/2/1
```

Related Commands

Command	Description
ftp client passive	Configures the software to use only passive FTP connections.

ping (network)

To check host reachability and network connectivity on IP networks, use the **ping** command in EXEC mode.

ping [**ipv4 | ipv6 | vrf** *vrf-name*] [*host-name* | *ip-address*] [**count** *number*] [**size** *number*] [**source** {*ip-address* | **type** *number*}] [**timeout** *seconds*] [**pattern** *number*] [**type** *number*] [**priority** *number*] [**verbose**] [**donnotfrag**] [**validate**] [**sweep**]

Syntax Description

ipv4	(Optional) Specifies IPv4 address prefixes.
ipv6	(Optional) Specifies IPv6 address prefixes.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **ipv4** and **ipv6** keywords were added.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added. A range was added for the **size** keyword.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Table 42 describes the test characters sent by the ping facility.

Table 42 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:

```
RP/0/RP0/CPU0: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:

```
RP/0/RP0/CPU0: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
```

rcp client source-interface

To specify the source IP address for remote copy protocol (rcp) connections, use the **rcp client source-interface** command in global configuration mode. To remove the **rcp client source-interface** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

rcp client source-interface *type instance*

no rcp client source-interface *type instance*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

The rcp source address is the IP address of the interface used by the rcp packets to leave the networking device.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **rcp client source-interface** command to set the IP address of an interface as the source for all rcp connections. To configure the remote username to be used when a remote copy using rcp is requested, use the **rcp client username** command.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to set the IP address for Packet-over-SONET (POS) interface 1/0/2/1 as the source address for rcp connections:

```
RP/0/RP0/CPU0:router(config)# rcp client source-interface POS 1/0/2/1
```

Related Commands

Command	Description
rcp client username	Configures the remote username to be used when a remote copy using rcp is requested.

rcp client username

To configure the local user on the client side to be used when requesting a remote copy using remote copy protocol (rcp), use the **rcp client username** command in global configuration mode. To restore the system to its default condition, use the **no** form of this command.

rcp client username *username*

no rcp client username *username*

Syntax Description

username	Name of the remote user on the rcp server. This name is used for rcp copy requests. If the rcp server has a directory structure, all files and images to be copied are searched for or written relative to the directory in the remote user account.

Defaults

If you do not issue this command, the software sends the remote username associated with the current tty process, if that name is valid, for rcp copy commands. For example, if the user is connected to the networking device through Telnet and the user was authenticated through the **username** command, the software sends that username as the remote username.

If the username for the current tty process is not valid, the software sends the hostname as the remote username. For rcp boot commands, the software sends the network server hostname by default.

Note For Cisco, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The rcp protocol requires that a client send the remote username on an rcp request to the network server. Use the **rcp client username** command to specify the remote username to be sent to the network server for an rcp copy request. If the network server has a directory structure, as do UNIX systems, all files and images to be copied are searched for or written relative to the directory in the remote user account. To specify a source address for rcp connections, use the **rcp client source-interface** command.

Note The remote username must be associated with an account on the destination server.

Task ID

Task ID	Operations
ip-services	read, write

Examples

The following example shows how to configure the remote username to netadmin1:

```
RP/0/RP0/CPU0:router(config)# rcp client username netadmin1
```

Related Commands

Command	Description
rcp client source-interface	Specifies the source IP address for rcp connections.

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 EXEC mode.

show cinetd services

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Family Service   Proto   Port   ACL  max_cnt  curr_cnt wait  Program Option
=============================================================================
v4     telnet    tcp      23 unlimited  0        nowait       telnet
v4     tftp      udp      69 unlimited  0        wait          tftpd   disk0
```

Table 43 describes the significant fields shown in the display.

Table 43 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.
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.

Related Commands

Command	Description
telnet ipv4 server	Enables Telnet services on a networking device.
tftp ipv4 server	Enables or disables the TFTP server or a feature running on the TFTP server.

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 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.

Defaults

Unicast address prefixes are the default when IPv4 address prefixes are configured.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ip-services	read

Examples

The following is sample output from the **show hosts** command:

```
RP/0/RP0/CPU0: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
```

Table 44 describes the significant fields shown in the display.

Table 44 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.
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.

Related Commands

Command	Description
clear host	Deletes entries from the host-name-and-address cache.
domain list	Defines a list of default domain names to complete unqualified hostnames.
domain lookup disable	Disables the IP DNS-based hostname-to-address translation.
domain name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
domain name-server	Specifies the address of one or more name servers to use for name and address resolution.

telnet

To log in to a host that supports Telnet, use the **telnet** command in EXEC mode.

telnet {*ip-address* | *host-name*} [*options*]

Syntax Description

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 Table 45 for a list of supported options.

Defaults

Telnet client is in telnet connection options nostream mode.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Table 45 lists the supported Telnet connection options.

Table 45 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. Table 46 lists the special Telnet escape sequences.

Table 46 Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ c	Interrupt Process (IP).
Ctrl-^ o	Abort Output (AO).
Ctrl-^ u	Erase Line (EL).

1. 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:

```
RP/0/RP0/CPU0: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:

```
RP/0/RP0/CPU0:router# telnet host1
```

Related Commands

Command	Description
aaa authentication login default local	Sets AAA authentication at login.
telnet dscp	Defines 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.
telnet server	Enables Telnet services on a networking device.
terminal length	Sets the number of lines on the current terminal screen for the current session.
terminal width	Sets the number of character columns on the terminal screen for the current session.

telnet client source-interface

To specify the source IP address for a Telnet connection, use the **telnet client source-interface** command in global configuration 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 instance*

no telnet client source-interface *type instance*

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.
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 (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.

Defaults

The IP address of the best route to the destination is used as the source IP address.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 Packet-over-SONET (POS) interface 1/0/2/1 as the source address for Telnet connections:

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 client source-interface POS 1/0/2/1
```

Related Commands

Command	Description
telnet server	Enable Telnet services on a networking device.

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 global configuration 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.

Defaults

If DSCP is disabled or not configured, the following default values are listed:

- The default value for the server is 16.
- The default value for the client is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router(config)# telnet vrf default ipv4 dscp 40
```

```
RP/0/RP0/CPU0:router(config)# telnet vrf default ipv4 dscp 10
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

telnet server

To enable Telnet services on a networking device, use the **telnet server** command in global configuration 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.

Defaults

Telnet services are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	The **vrf** and **default** keywords and *vrf-name* argument were added.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 Guide, System Management Configuration Guide, and IP Addresses and Services Configuration Guide).

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:

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers 1
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

telnet transparent

To send a CR (carriage return) as a CR-NULL rather than a CR-LF (carriage return-line feed) 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 arguments or keywords.

Command Modes

Line console

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router(config)# line console
RP/0/RP0/CPU0:router(config-line)# telnet transparent
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

tftp client source-interface

To specify the source IP address for a TFTP connection, use the **tftp client source-interface** command in global configuration 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 instance*

no tftp client source-interface *type instance*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

The IP address of the best route to the destination is used as the source IP address.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 Packet-over-SONET (POS) interface 1/0/2/1 as the source address for TFTP connections:

```
RP/0/RP0/CPU0:router(config)# tftp client source-interface POS 1/0/2/1
```

Related Commands

Command	Description
tftp server	Enables the TFTP server to start or stop listening for TFTP connections.

tftp server

To enable or disable the TFTP server or a feature running on the TFTP server, use the **tftp server** command in global configuration mode. To restore the system to its default condition, use the **no** form of this command.

tftp {**ipv4** | **ipv6**} **server** {**homedir** *tftp-home-directory*} [**max-servers** *number*] [**access-list** *name*]

no tftp {**ipv4** | **ipv6**} **server** {**homedir** *tftp-home-directory*} [**max-servers** *number*] [**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. Range is 1 to 2147483647.
access-list *name*	(Optional) Specifies the name of the access list associated with the TFTP server.

Defaults

The TFTP server is disabled by default. When not specified, the default value for the **max-servers** keyword is unlimited.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **max-servers** *number* keyword and argument are now optional.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 access-list test homedir disk0
```

Related Commands

Command	Description
show cinetd services	Displays the services whose processes are spawned by cinetd.

traceroute

To discover the routes that packets actually take when traveling to their destination across an IP network, use the **traceroute** command in EXEC mode.

traceroute [**ipv4 | ipv6 | vrf** *vrf-name*] [*host-name* | *ip-address*] [**source** *ip-address-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.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) VRF name of the system to ping.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Common Trace Problems

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, **traceroute** 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:

```
RP/0/RP0/CPU0: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:

```
RP/0/RP0/CPU0:router# 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  stc15-001ab-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
```

Table 47 describes the characters that can appear in traceroute output.

Table 47 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.

HSRP Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure and monitor the Hot Standby Router Protocol (HSRP).

For detailed information about HSRP concepts, configuration tasks, and examples, refer to the *Implementing HSRP on Cisco IOS XR Software* configuration module.

hsrp authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **hsrp authentication** command in HSRP interface configuration mode. To delete an authentication string, use the **no** form of this command.

hsrp [*group-number*] **authentication** *string*

no hsrp [*group-number*] **authentication** [*string*]

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies. Default is 0.
string	Authentication string. It can be up to eight characters long. Default string is cisco.

Defaults

group-number: 0
string: cisco

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a LAN to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP. Authentication mismatch does not prevent protocol events such as one router taking over as the designated router.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to configure “company1” as the authentication string required to allow Hot Standby routers in group 1 on Ten Gigabit Ethernet interface 0/2/0/1 to interoperate:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 authentication company1
```

Related Commands

Command	Description
show hsrp	Displays HSRP information.

hsrp delay

To configure the activation delay for the Hot Standby Router Protocol (HSRP), use the **hsrp delay** command in HSRP interface configuration mode. To delete the activation delay, use the **no** form of this command.

hsrp delay {**minimum** *value* **reload** *value*}

no hsrp delay

Syntax Description

minimum *value*	Sets the minimum delay in seconds for every interface up event. Range is 1 to 10000.
reload *value*	Sets the reload delay in seconds for first interface up event. Range is 1 to 10000.

Defaults

minimum *value*: 1
reload *value*: 1

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hsrp delay** command delays the start of the HSRP finite state machine (FSM) on an interface up event to ensure that the interface is ready to pass traffic. This ensures that there are no mistaken state changes due to loss of hello packets. The minimum delay is applied on all interface up events and the reload delay is applied on the first interface event.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to configure a minimum delay of 10 seconds with a reload delay of 100 seconds:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface mgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp delay minimum 10 reload 100
```

Related Commands

Command	Description
show hsrp	Displays HSRP information.

hsrp ipv4

To activate the Hot Standby Router Protocol (HSRP), use the **hsrp ipv4** command in HSRP interface configuration mode. To disable HSRP, use the **no** form of this command.

hsrp [*group-number*] **ipv4** [*ip-address* [**secondary**]]

no hsrp [*group-number*] **ipv4** [*ip-address* [**secondary**]]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. Range is 0 to 255. Default is 0.
ip-address	(Optional) IP address of the Hot Standby router interface.
secondary	(Optional) Indicates that the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

Defaults

group-number: 0
HSRP is disabled by default.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hsrp ipv4** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the virtual address is learned from the active router. For HSRP to elect a designated router, at least one router in the Hot Standby group must have been configured with, or must have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

When the **hsrp ipv4** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). If the Hot Standby state group has been configured with or has learned the designated address, the proxy ARP requests are answered using the MAC address of the Hot Standby group. Otherwise, proxy ARP responses are suppressed.

Configuring secondary Hot Standby router IP addresses is necessary when the interface has secondary IP addresses configured and redundancy must be provided for the networks of these addresses also.

A primary address must be configured before a secondary address. Likewise, a secondary address must be unconfigured before unconfiguring a primary address. All IP addresses can be unconfigured using the **no hsrp ipv4** command.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to activate HSRP for group 1 on Ten Gigabit Ethernet interface 0/2/0/1. The IP address used by the Hot Standby group is learned using HSRP.

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4
```

Related Commands

Command	Description
hsrp redirects	Configures ICMP redirect messages to be sent when the HSRP is configured on an interface.
show hsrp	Displays HSRP information.

hsrp mac-address

To specify a virtual MAC address for the Hot Standby Router Protocol (HSRP), use the **hsrp mac-address** command in HSRP interface configuration mode. To revert to the standard virtual MAC address (0000.0C07.AC*n)*, use the **no** form of this command.

hsrp [*group-number*] **mac-address** *address*

no hsrp [*group-number*] **mac-address**

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. Default is 0.
address	MAC address.

Defaults

group-number: 0

If this command is not configured, and the **hsrp use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*n*, where *n* is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hsrp mac-address** command is not recommended except for IBM networking environments in which first-hop redundancy is based on being able to use a virtual MAC address and in which you cannot change the first-hop addresses in the PCs that are connected to an Ethernet switch.

HSRP is used to help end stations locate the first-hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first-hop for routing purposes. In this case, it is often necessary to specify the virtual MAC address; the virtual IP address is unimportant for these protocols.

Use the **hsrp mac-address** command to specify the virtual MAC address. The MAC address specified is used as the virtual MAC address when the router is active. This command is intended for certain APPN configurations.

Table 48 shows the parallel terms between APPN and IP.

Table 48 APPN and IP Parallel Terms

APPN	IP
end node	host
network node	router or gateway

Note In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **hsrp mac-address** command in the routers to set the virtual MAC address to the value used in the end nodes.

Task ID

Task ID	Operations
hsrp	read, write

Examples

If the end nodes are configured to use 4000.1000.1060 as the MAC address of the network node, the command to configure the virtual MAC address is as follows:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 5 mac-address 4000.1000.1060
```

Related Commands

Command	Description
hsrp use-bia	Configures HSRP to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address.
show hsrp	Displays HSRP information.

hsrp preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **hsrp preempt** command in HSRP interface configuration mode. To restore the default values, use the **no** form of this command.

hsrp [*group-number*] **preempt** [**delay** *seconds*]

no hsrp [*group-number*] **preempt** [**delay** *seconds*]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply. Default is 0.
delay *seconds*	(Optional) Time in seconds. The *seconds* argument causes the local router to postpone taking over the active role for the specified preempt delay *seconds* value. Range is 0 to 3600 seconds (1 hour). Default is 0 seconds (no delay).

Defaults

group-number: 0
seconds: 0 seconds (if the router wants to preempt, it does immediately)

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When the **hsrp preempt** command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If the **hsrp preempt** command is not configured, the local router assumes control as the active router only if it receives information indicating that no router is currently in the active state (acting as the designated router).

When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, yet it is unable to provide adequate routing services. This problem can be solved by configuring a delay before the preempting router actually preempts the currently active router.

The preempt delay *seconds* value does not apply if there is no router currently in the active state. In this case, the local router becomes active after the appropriate timeouts (see the **hsrp timers** command), regardless of the preempt *delay seconds* value.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, the router waits for 300 seconds (5 minutes) after having determined that it should preempt before attempting to preempt the active router. The router might become the active router despite the delay, if no active router is present. Only preempting the active router is delayed.

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp ipv4 172.19.108.254
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp preempt delay 300
```

Related Commands

Command	Description
hsrp priority	Configures HSRP priority.
hsrp track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
show hsrp	Displays HSRP information.

hsrp priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **hsrp priority** command in HSRP interface configuration mode. To restore the default values, use the **no** form of this command.

hsrp [*group-number*] **priority** *priority*

no hsrp [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the priority applies. Default is 0.
priority	Priority value that prioritizes a potential Hot Standby router. Range is 1 to 255. Default is 100.

Defaults

group-number: 0
priority: 100

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

The priority of the device can change dynamically if an interface is configured with the **hsrp track** command and another interface on the device goes down.

If preemption is not enabled, the router may not become active even though it might have a higher priority than other HSRP routers.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, the router has a priority of 120:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp ipv4 172.19.108.254
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp priority 120
```

Related Commands

Command	Description
hsrp preempt	Configures HSRP preemption and preemption delay.
hsrp track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
show hsrp	Displays HSRP information.

hsrp redirects

To configure Internet Control Message Protocol (ICMP) redirect messages to be sent when the Hot Standby Router Protocol (HSRP) is configured on an interface, use the **hsrp redirects** command in HSRP interface configuration mode. To revert to the default, which is that ICMP messages are enabled, use the **no** form of this command.

hsrp redirects disable

no hsrp redirects disable

Syntax Description

disable	Disables the filtering of ICMP redirect messages on interfaces configured with HSRP.

Defaults

HSRP ICMP redirects are enabled by default.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **disable** keyword was made mandatory.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hsrp redirects** command can be configured on a per-interface basis. When HSRP is first configured on an interface, the setting for that interface inherits the global value.

With the **hsrp redirects** command enabled, ICMP redirects messages are filtered by replacing the real IP address in the next-hop address of the redirect packet with a virtual IP address if it is known to HSRP.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to allow HSRP to filter redirect messages on Ten Gigabit Ethernet interface 0/2/0/1:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4 172.16.0.1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp redirects disable
```

Related Commands

Command	Description
show hsrp	Displays HSRP information.

hsrp timers

To configure the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down, use the **hsrp timers** command in HSRP interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

hsrp [*group-number*] **timers** {*hello-seconds* | **msec** *hello-milliseconds*} {*hold-seconds* | **msec** *hold-milliseconds*}

no hsrp [*group-number*] **timers**

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply. Default is 0.
hello-seconds	Hello interval in seconds. Range is 1 to 255. Default is 3 seconds.
msec *hello-milliseconds*	Hello interval in milliseconds. Range is 20 to 3000 milliseconds.
hold-seconds	Time in seconds before the active or standby router is declared to be down. Range is 1 to 255. Default is 10 seconds.
msec *hold-milliseconds*	Time in milliseconds before the active or standby router is declared to be down. Range is 20 to 3000 milliseconds.

Defaults

group-number: 0
hello-seconds: 3 seconds (If the **msec** keyword is specified, there is no default value.)
hold-seconds: 10 seconds (If the **msec** keyword is specified, there is no default value.)

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Nonactive routers learn timer values from the active router, unless millisecond timer values are being used. If millisecond timer values are being used, all routers must be configured with the millisecond timer values. This rule applies if either the hello time or the hold time is specified in milliseconds.

The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, the hold time is greater than or equal to three times the hello time (holdtime ≥ 3 * hellotime).

You must specify either the *hello-seconds* argument or the **msec** keyword and *hello-milliseconds* argument, depending on whether you want the hello time in seconds or milliseconds. You must also specify either the *hold-seconds* argument or **msec** keyword and *hold-milliseconds* argument, depending on whether you want the hold time in seconds or milliseconds.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to set, for group number 1 on Ten Gigabit Ethernet interface 0/2/0/1, the time between hello packets to 5 seconds and the time after which a router is considered to be down to 15 seconds. The configured timer values are used only if the router is active (or before they have been learned).

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 timers 5 15
```

The following example shows how to set, for group number 1 on Ten Gigabit Ethernet interface 0/2/0/1, the time between hello packets to 200 milliseconds and the time after which a router is considered to be down to 1000 milliseconds. The configured timer values are always used because milliseconds have been specified.

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 timers msec 200 msec 1000
```

Related Commands

Command	Description
show hsrp	Displays HSRP information.

hsrp track

To configure an interface so that the Hot Standby priority changes on the basis of the availability of other interfaces, use the **hsrp track** command in HSRP interface configuration mode. To remove the tracking, use the **no** form of this command.

hsrp [*group-number*] **track interface** *type instance* [*priority-decrement*]

no hsrp [*group-number*] **track interface** *type instance* [*priority-decrement*]

Syntax Description

group-number	(Optional) Group number on the interface to which the tracking applies. Default is 0.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
priority-decrement	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). Range is 1 to 255.

Defaults

group-number: 0
priority-decrement: 10

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **hsrp track** command ties the Hot Standby priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for the Hot Standby Router Protocol (HSRP). Only IP interfaces are tracked. A tracked interface is up if IP on that interface is up. Otherwise, the tracked interface is down.

When a tracked interface goes down, the Hot Standby priority decreases by 10. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each interface configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

The optional *priority-decrement* argument specifies by how much to decrement the Hot Standby priority when a tracked interface goes down. When the tracked interface comes back up, the priority is incremented by the same amount.

When multiple tracked interfaces are down and *priority-decrement* values have been configured, these configured priority decrements are cumulative. If tracked interfaces are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative.

The **hsrp preempt** command must be used in conjunction with this command on all routers in the group whenever the best available router should be used to forward packets. If the **hsrp preempt** command is not used, then the active router stays active, regardless of the current priorities of the other HSRP routers.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, Ten Gigabit Ethernet interface 0/2/0/1 tracks interface 0/1/0/1 and 0/3/0/1. If one or both of these two interfaces go down, the Hot Standby priority of the router decreases by 10. Because the default Hot Standby priority is 100, the priority becomes 90 when one of the tracked interfaces goes down and the priority becomes 80 when both go down.

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp track TenGigE 0/1/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp track TenGigE 0/3/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp preempt
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp ipv4 192.92.72.46
```

Related Commands

Command	Description
hsrp preempt	Configures HSRP preemption and preemption delay.
hsrp priority	Configures HSRP priority.
show hsrp	Displays HSRP information.

hsrp use-bia

To configure the Hot Standby Router Protocol (HSRP) to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address or the functional address, use the **hsrp use-bia** command in HSRP interface configuration mode. To restore the default virtual MAC address, use the **no** form of this command.

hsrp use-bia

no hsrp use-bia

Syntax Description

This command has no arguments or keywords.

Defaults

HSRP uses the preassigned MAC address on Ethernet.

Command Modes

HSRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

It is desirable to configure the **hsrp use-bia** command on an interface if there are devices that reject Address Resolution Protocol (ARP) replies with source hardware addresses set to a functional address.

Task ID

Task ID	Operations
hsrp	read, write

Examples

In the following example, the burned-in address of Ten Gigabit Ethernet interface 0/2/0/1 will be the virtual MAC address mapped to the virtual IP address for all Hot Standby groups configured on Ten Gigabit Ethernet interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp use-bia
```

Related Commands

Command	Description
hsrp mac-address	Specifies a virtual MAC address for HSRP.
show hsrp	Displays HSRP information.

interface (HSRP)

To enable Hot Standby Router Protocol (HSRP) interface configuration command mode, use the **interface** command in router configuration mode. To terminate interface mode, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

HSRP is disabled.

Command Modes

Router HSRP configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

All the commands used to configure HSRP are used in HSRP interface configuration mode.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example show how to enable HSRP interface configuration mode on Ten Gigabit Ethernet interface 0/2/0/1:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)#
```

Related Commands

Command	Description
router hsrp	Enables HSRP.

router hsrp

To enable the Hot Standby Router Protocol (HSRP), use the **router hsrp** command in global configuration mode. To disable HSRP, use the **no** form of this command.

router hsrp

no router hsrp

Syntax Description

This command has no arguments or keywords.

Defaults

HSRP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

HSRP configuration commands must be configured in the HSRP interface configuration mode.

Task ID

Task ID	Operations
hsrp	read, write

Examples

The following example shows how to configure an HSRP redundancy process that contains a virtual router group 1 on Ten Gigabit Ethernet interface 0/2/0/1:

```
RP/0/RP0/CPU0:router(config)# router hsrp
RP/0/RP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RP0/CPU0:router(config-hsrp-if)# hsrp 1 priority 254
```

show hsrp

To display Hot Standby Router Protocol (HSRP) information, use the **show hsrp** command in EXEC mode.

show hsrp [**interface** *type instance*] [*group-number*]] [**brief** | **detail** |]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
group-number	(Optional) Group number on the interface for which output is displayed.
brief	(Optional) A single line of output summarizes each standby group. The **brief** keyword is the default if **detail** is not specified.
detail	(Optional) This keyword has the same effect as not specifying **brief**; more output is provided.
|	(Optional) After this vertical bar (|), specify one of the following output modifiers and a keyword from the output: • **begin**—Begins the output from the word that you specify. • **exclude**—Excludes lines that match the word that you specify. • **include**—Includes lines that match the word that you specify.

Defaults

The **brief** keyword is the default.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show hsrp** command to display HSRP information.

If you want to specify a value for the *group-number* argument, you must also specify an interface *type* and *number*.

Task ID

Task ID	Operations
hsrp	read

Examples

The following is sample output from the **show hsrp detail** command:

```
RP/0/RP0/CPU0:router# show hsrp detail

GigabitEthernet0/4/0/0 - Group 1
  Local state is Active, priority 100
  Hellotime 3 sec holdtime 10 sec
  Next hello sent in 0.539
  Minimum delay 1 sec, reload delay 5 sec
  Hot standby IP address is 4.0.0.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac01
  2 state changes, last state change 00:05:20
```

Table 49 describes the significant fields shown in the display.

Table 49 show hsrp Command Field Descriptions

Field	Description
TenGigE0/2/0/4	Interface type and number and Hot Standby group number for the interface.
Local state is	State of local networking device; can be one of the following: • Active—Current Hot Standby router. • Standby—Router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither active nor standby, but if no messages are received from the active or standby router, it will start to "speak." • Learn—Router is neither active nor standby, nor does it have enough information to attempt to claim the active or standby roles. • Init—Router is not yet ready to participate in HSRP, possibly because the associated interface is not up.
Hellotime	Current time (in seconds) between sending of hello packets, learned dynamically from the hello packets received from the active Hot Standby router.
holdtime	Current time (in seconds) before other routers declare the active or standby router to be down, learned dynamically from the hello packets received from the active Hot Standby router.
Next hello sent in	Time in which the software will send the next hello packet (in hours:minutes:seconds).
Hot standby IP address is configured	IP address of the current Hot Standby router. The word "configured" indicates that this address is known through the **hsrp ip** command. Otherwise, the address was learned dynamically through HSRP hello packets from other routers that do have the HSRP IP address configured.
Active router is	Value can be "local" or an IP address. Address of the current active Hot Standby router.
Standby router is	Value can be "local" or an IP address of the standby router (the router that is next in line to be the Hot Standby router).
Standby virtual mac address is	MAC address associated with the standby group address.
state changes	Number of times the router changed the standby state.
last state change	Time (in hours:minutes:seconds) expired since the last state change.
Tracking interface states for	List of interfaces that are being tracked and their corresponding states. Based on the **hsrp track** command.
Priority decrement	Value by which the standby priority is decremented or incremented when the tracked interface goes down or up, respectively. Default is 10.

Related Commands

Command	Description
hsrp authentication	Configures an authentication string for HSRP.
hsrp delay	Configures the activation delay for the HSRP.

Command	Description
hsrp ipv4	Activates the HSRP.
hsrp mac-address	Specifies a virtual MAC address for HSRP.
hsrp preempt	Configures HSRP preemption and preemption delay.
hsrp priority	Configures HSRP priority.
hsrp timers	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.
hsrp track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
hsrp use-bia	Configures HSRP to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address.

LPTS Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR commands used to monitor Local Packet Transport Services (LPTS).

clear lpts ifib statistics

To clear the Internal Forwarding Information Base (IFIB) statistics, use the **clear lpts ifib statistics** command in EXEC mode.

clear lpts ifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Clears the IFIB statistics for the designated node. The *node-id* argument is entered in standard *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you do not specify a node with the **location** keyword and *node-id* argument, this command clears the IFIB statistics for the node on which the command is run.

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
```

Related Commands

Command	Description
show lpts ifib statistics	Displays the 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 EXEC mode.

clear lpts pifib statistics [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Clears the Pre-IFIB statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you do not specify a node with the **location** keyword and *node-id* argument, this command clears the Pre-IFIB statistics for the node on which the command is run.

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
```

Related Commands

Command	Description
show lpts pifib statistics	Displays the LPTS PIFIB statistics.

show lpts bindings

To display the binding information in the Port Arbitrator, use the **show lpts bindings** command in EXEC mode.

show lpts bindings [**location** *node-id*] [**client-id** {**clnl** | **ipsec** | **ipv4-io** | **ipv6-io** | **mpa** | **tcp** | **test** | **udp** | **raw**}] [**brief**]

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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output 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
```

Table 50 describes the significant fields shown in the display.

Table 50 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.

Table 50 show lpts bindings Command Field Descriptions (continued)

Field	Description
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 is sample output 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
```

Table 51 describes the significant fields shown in the display.

Table 51 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.

Related Commands

Command	Description
show lpts clients	Displays the client information for the Port Arbitrator.
show lpts flows	Displays information about LPTS flows.

show lpts clients

To display the client information for the Port Arbitrator, use the **show lpts clients** command in EXEC mode.

show lpts clients [**times**]

Syntax Description

times	(Optional) Displays information about binding request rates and service times.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output 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
```

Table 52 describes the significant fields shown in the display.

Table 52 show lpts clients Command Field Descriptions

Field	Description
Clid	LPTS client ID.
Loc	Node location, in the format *rack/slot/module*.
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 is sample output 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
```

Related Commands

Command	Description
show lpts bindings	Displays the binding information in the port arbitrator.
show lpts flows	Displays information about LPTS flows.

show lpts flows

To display information about Local Packet Transport Services (LPTS) flows, use the **show lpts flows** command in EXEC mode.

show lpts flows [**brief**]

Syntax Description

brief	(Optional) Displays summary output.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output 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
```

Table 53 describes the significant fields shown in the display.

Table 53 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. Ant 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 is sample output 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
```

Table 54 describes the significant fields shown in the display.

Table 54 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.

Related Commands

Command	Description
show lpts bindings	Displays the binding information in the port arbitrator.
show lpts clients	Displays the client information for the port arbitrator.

show lpts ifib

To display the entries in the Internal Forwarding Information Base (IFIB), use the **show lpts ifib** command in 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**]]

Syntax Description

entry	(Optional) Displays IFIB entries.
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	All IFIB types.
brief	(Optional) IFIB entries in brief format.
statistics	(Optional) IFIB table with statistics information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output from the **show lpts ifib** command:

```
RP/0/RP1/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/EIGRP/IPv4_STACK/0/0/0
Deliver List     : 0/5/CPU0
-----------------------------------------------------
```

Table 55 describes the significant fields shown in the display.

Table 55 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.

Table 55 show lpts ifib entries Command Field Descriptions (continued)

Field	Description
Interface	Ingress interface name.
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 is sample output 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 is sample output 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
```

Related Commands

Command	Description
show lpts ifib slices	Displays IFIB slice information.

show lpts ifib slices

To display Internal Forwarding Information Base (IFIB) slice information, use the **show lpts ifib slices** command in 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) All entries.
statistics	(Optional) Statistics for slice lookups.
times	(Optional) IFIB update transaction times.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 is sample output 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/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
```

The following is sample output 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/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/RP1/CPU0:
   total:5 tx 13 upd 1/-/1ms/tx
```

The following is sample output 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
```

Table 56 describes the significant fields shown in the display.

Table 56 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*.

Related Commands

Command	Description
show lpts ifib	Displays entries in the IFIB.

show lpts ifib statistics

To display Internal Forwarding Information Base (IFIB) statistics, use the **show lpts ifib statistics** command in EXEC mode.

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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output from the **show lpts ifib statistics** command:

```
RP/0/RP0/CPU0:router# show lpts ifib statistics

Flow Manager 0/RP1/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
```

Table 57 describes the significant fields shown in the display.

Table 57 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.
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.

Related Commands

Command	Description
show lpts ifib	Displays the entries in an IFIB slice.

show lpts ifib times

To display Internal Forwarding Information Base (IFIB) update transaction times, use the **show lpts ifib times** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output 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/RP1/CPU0:
 total:5 tx 13 upd 1/-/1ms/tx
```

Table 58 describes the significant fields shown in the display.

Table 58 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*.

Related Commands

Command	Description
show lpts ifib	Displays detailed information about entries in an IFIB slice.

show lpts mpa groups

To display aggregate information about multicast bindings for groups, use the **show lpts mpa groups** command in EXEC mode.

show lpts mpa groups interface *type instance*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

No default behavior or values

Command Types

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show lpts mpa groups** command is used to aggregate information about the multicast groups joined on a specified interface. This command also displays the filter mode and source list associated with the groups joined on a specified interface.

Task ID

Task ID	Operations
lpts	read
network	read

Examples

The following is sample output from the **show lpts mpa groups** command:

```
RP/0/RP0/CPU0:router# show lpts mpa groups POS 0/0/0/0

  224.0.0.2 : 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>
```

Table 59 describes the significant fields shown in the display.

Table 59 show lpts mpa groups Command Field Descriptions

Field	Description
Includes	Displays the number of sockets that have set up an INCLUDE mode filter for that group and if there are any source-specific filters.
Excludes	Displays the number of sockets that have set up an EXCLUDE mode filter for that group and if there are any source-specific filters.

show lpts pifib

To display Pre-Internal Forwarding Information Base (Pre-IFIB) entries, use the **show lpts pifib** command in EXEC mode.

show lpts pifib [**entry**] [**type** {**isis** | **ipv4** {**frag** | **ixmp** | **mcast** | **tcp** | **udp** | **ipsec** | **raw**} | **ipv6** {**frag** | **icmp** | **ixmp** | **mcast** | **tcp** | **udp** | **ipsec** | **raw** } | **all**}] [**brief** [**statistics**] [**location** *node-id*]

Syntax Description

entry	(Optional) Pre-IFIB entry.
type	(Optional) Protocol type.
isis	Intermediate System-to-Intermediate System (IS-IS) sub Pre-IFIB type.
ipv4	IPv4 sub Pre-IFIB type. Possible values include **frag**, **ixmp**, **mcast**, **tcp**, **udp**, **ipsec**, and **raw**.
ipv6	IPv6 sub Pre-IFIB type. Possible values include **frag**, **icmp**, **ixmp**, **mcast**, **tcp**, **udp**, **ipsec, and raw**.
frag	IPv4 or IPv6 fragment.
icmp	IPv4 or IPv6 IXMP and Internet Group Management Protocol (IGMP).
ixmp	IPv4 or IPv6 IXMP (ICMP and Internet Group Management Protocol [IGMP]).
mcast	IPv4 or IPv6 Multicast.
tcp	IPv4 or IPv6 Transmission Control Protocol (TCP).
udp	IPv4 or IPv6 User Datagram Protocol (UDP).
ipsec	Secure IP.
raw	IPv4 orIPv6 raw IP.
all	All sub Pre-IFIBs.
brief	(Optional) Pre-IFIB entries in brief format.
statistics	(Optional) Pre-IFIB table with statistics information.
location *node-id*	(Optional) The *node-id* argument is entered in the *rack/slot/module* notation (for example, 0/7/CPU0).

Defaults

By default, all entries are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 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

O - Opcode; F - Flow Type; L - Listener Tag; I - Local Flag; T - Min TTL;
na - Not Applicable
-----------------------------------------------------
L3 Protocol       : CLNS
L4 Protocol       : -
VRF-ID            : default (0x60000000)
Destination IP    : any
Source IP         : any
Port/Type         : any
Source Port       : any
Is Fragment       : 0
Is SYN            : 0
Interface         : any (0x0)
O/F/L/I/T         : DELIVER/ISIS-default/CLNS_STACK/0/0
Deliver List      : FGID 11935
Accepts/Drops     : 0/0
Is Stale          : 0
```

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 entry brief** 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 *        224.0.0.5 any             any   any          0/0/CPU0
 IPv4_mcast *        224.0.0.6 any             any   any          0/0/CPU0
 IPv4_mcast *        224.0.0.0/4 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 is sample output from the **show lpts pifib entry brief statistics** command:

```
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
```

Table 60 describes the significant fields shown in the display for the **show lpts pifib brief statistics** command.

Table 60 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.
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 EXEC mode.

show lpts pifib hardware entry [**type** {**ipv4** | **ipv6** | **isis**}] [**start-index** *number* **num-entries** *number*] [**brief** | **statistics**] [**location** *node-id*]

Syntax Description

type	(Optional) Specifies the hardware entry type. Enter one of the following types: • **ipv4**—Specifies IPv4 entries. • **ipv6**—Specifies IPv6 entries. • **isis**—Specifies ISIS entries.
start-index *number*	(Optional) Starting index number.
num-entries *number*	(Optional) Maximum entries permitted.
brief	(Optional) Displays summary hardware entry information.
statistics	(Optional) Displays hardware entry accept/drop statistics for each summary entry.
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.

Defaults

Displays brief hardware entry information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output from the **show lpts pifib hardware entry** command with the **location** keyword:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware entry location 0/1/CPU0

             Node: 0/1/CPU0:
----------------------------------------
V - Vital; M - Fabric Multicast;
C - Moose Congestion Flag; L - Listener Tag; T - Min TTL;
F - Flow Type;
DestNode - Destination Node;
DestAddr - Destination Fabric Address;
Sq - Ingress Shaping Queue; Dq - Destination Queue;
Po - Policer; Ct - Stats Counter;
Lp - Lookup priority; Sp - Storage Priority;
Ar - Average rate limit; Bu - Burst;
Rsp - Relative sorting position;
----------------------------------------------------
L4 Protocol       : any
VRF ID            : any
Source IP         : any
Port/Type         : any
Source Port       : any
Is Fragment       : 1
Is SYN            : any
Interface         : any
V/M/C/L/T/F       : 0/0/0/IPv4_REASS/0/Fragment
DestNode          : Local
DestAddr          : Punt
Sq/Dq/Ct          : 4/na/0x24400
Accepted/Dropped  : 0/0
Lp/Sp             : 0/0
# of TCAM entries : 1
Po/Ar/Bu          : 101/1000pps/100ms
State             : Entry in TCAM
Rsp/Rtp           : 0/0
----------------------------------------------------
```

Table 61 describes the significant fields shown in the display.

Table 61 show lpts pifib hardware entry Command Field Descriptions

Field	Description
L4 Protocol	Layer 4 protocol of the entry.
VRF ID	VPN routing and forwarding (VRF) identification (vrfid) number.
Source IP	Source IP address for this entry.
Port/Type	Port or ICMP[1] type for this entry.
Source Port	Source port for this entry.
Is Fragment	Indicates if this entry applies to IP fragments.
Is SYN	Indicates if this entry applies to TCP SYNs.
Interface	Interface for this entry.

Table 61 show lpts pifib hardware entry Command Field Descriptions (continued)

Field	Description
V/M/C/L/T/F	• V—vital • M—fabric multicast • C—moose congestion flag • L—listener tag • T—minimum time-to-live • F—flow type
DestNode	Destination node to which to send the packet.
DestAddr	Destination address to which to send the packet.
Sq/Dq/Ct	• Sq—Ingress Shaping Queue • Dq—Destination Queue • Ct—Stats Counter.
Accepted/Dropped	Number of packets sent to DestAddr/Number of packets dropped due to policing.

1. Internet Control Message Protocol

show lpts pifib hardware usage

To display hardware table usage, use the **show lpts pifib hardware usage** command in EXEC mode.

show lpts pifib hardware usage [**type** {**ipv4** | **ipv6** | **isis**}] [**location** *node-id*]

Syntax Description

type	(Optional) Specifies the hardware entry type. Enter one of the following types: • **ipv4**—Specifies IPv4 entries. • **ipv6**—Specifies IPv6 entries. • **isis**—Specifies ISIS entries.
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.

Defaults

Without the optional parameters, the **show lpts pifib hardware usage** command displays a brief summary of hardware entry information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output from the **show lpts pifib hardware usage** command with the **location** keyword:

```
RP/0/RP0/CPU0:router# show lpts pifib hardware usage location 0/1/cpu0

Type       Size            Used            Used(%)
---------- --------------- --------------- -------
ipv4       6000            21              0.35
```

```
ipv6        4000            15              0.38
isis        4000            1               0.03
```

Table 62 describes the significant fields shown in the display.

Table 62 show lpts pifib hardware usage Command Field Descriptions

Field	Description
Type	Type of pre-IFIB entry.
Size	Maximum number of entries (72-bits) allowed for the type.
Used	Number of entries in use.
Used(%)	Percentage of total entries in use.

show lpts pifib statistics

To display Pre-Internal Forwarding Information Base (Pre-IFIB) statistics, use the **show lpts ifib statistics** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output 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
```

Table 63 describes the significant fields shown in the display.

Table 63 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.

Related Commands

Command	Description
show lpts pifib	Displays information about pre-IFIB entries.

show lpts port-arbitrator statistics

To display local packet transport services (LPTS) port arbitrator statistics, use the **show lpts port-arbitrator statistics** command in EXEC mode.

show lpts port-arbitrator statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output 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 lpts VPN router and forwarding (VRF) instance identification numbers and names, use the **show lpts vrf** command in EXEC mode.

show lpts vrf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
lpts	read

Examples

The following is sample output from the **show lpts vrf** command:

```
RP/0/RP0/CPU0:router# show lpts vrf

VRF-ID      VRF-NAME
0x00000000  *
0x60000000  default
```

Table 64 describes the significant fields shown in the display.

Table 64 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 IPv4 and IPv6 Commands on Cisco IOS XR Software

This chapter describes the commands available in the Cisco IOS XR software to 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 *Implementing Network Stack IPv4 and IPv6 on Cisco IOS XR Software* configuration module.

clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries, use the **clear ipv6 neighbors** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 POS 0/0/0/0
```

```
8888::8 - 1234.2345.9877 REACH POS0 /0/0/0
fe80::205:1ff:fe9f:6400 1335 0005.019f.6400 STALE POS 0/0/0/0
fe80::206:d6ff:fece:3808 1482 0006.d6ce.3808 STALE POS 0/0/0/0
fe80::200:11ff:fe11:1112 1533 0000.1111.1112 STALE POS 0/2/0/2

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 POS 0/0/0/0
8888::8 - 1234.2345.9877 REACH POS 0/0/0/0
fe80::205:1ff:fe9f:6400 1387 0005.019f.6400 STALE POS 0/0/0/0
fe80::206:d6ff:fece:3808 1534 0006.d6ce.3808 STALE POS 0/0/0/0
```

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 global configuration 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.

Defaults

The default value is one ICMP destination unreachable message every 500 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 rate of the ICMP destination unreachable message to one message every 10 milliseconds:

```
RP/0/RP0/CPU0:router(config)# icmp ipv4 rate-limit unreachable 10
```

ipv4 address

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**]

no ipv4 address *ipv4-address mask* [**secondary**]

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.

Defaults

No IPv4 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

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 POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
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
```

Related Commands

Command	Description
show ipv4 interface	Lists a summary of IPv4 information and status for the interface.

ipv4 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv4 conflict-policy** command in global configuration 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.

Defaults

Default is the lowest rack/slot if no conflict policy is configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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)# ipv6 conflict-policy static
```

Related Commands

Command	Description
show arm conflicts	Displays the IPv4 or IPv6 address conflict information.

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 arguments or keywords.

Defaults

By default, directed broadcasts are dropped.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv4 directed-broadcast
```

Related Commands

Command	Description
show ipv4 interface	Displays statistics for all interfaces configured for IPv4.
show ipv4 interface	Lists a summary of IPv4 information and status for the interface.
ipv4 unnumbered (point-to-point)	Enables IP processing on a point-to-point interface without assigning an explicit IP address to the interface.

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.

Defaults

IPv4 helper addresses are disabled. Default vrf is assumed if the vrf is not specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use this command with the **forward-protocol udp** command in global configuration 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.

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 POS interface 0/1/1/0 are forwarded to 192.168.1.0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv4 helper-address 192.168.1.0
```

Related Commands

Command	Description
forward-protocol udp	Specifies which ports the networking device forwards to when forwarding broadcast packets.

ipv4 mask-reply

To enable the Cisco IOS XR 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 arguments or keywords.

Defaults

IPv4 mask replies are not sent.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command enables the Cisco IOS XR 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 POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
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.

Defaults

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 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The router will fragment any IPv4 packet that exceeds the MTU set for the interface.

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

Examples

The following example shows how to set the maximum IPv4 packet size for POS interface 0/1/1/0 to 300 bytes:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv4 mtu 300
```

Related Commands

Command	Description
show ipv4 interface	Displays the MTU status of interfaces configured for IPv4.

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 arguments or keywords.

Defaults

ICMP redirect messages are disabled by default on the interface unless the Hot Standby Router Protocol (HSRP) is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If HSRP is configured on an interface, ICMP redirect messages are disabled by default on that 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 POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
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 global configuration 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 arguments or keywords.

Defaults

The software discards any IPv4 datagrams containing a source-route header option.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The following sections were modified: • Command description • Defaults • Usage Guidelines

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 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 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 (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.

Defaults

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 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

- Packet-over-SONET (POS) interfaces using High-Level Data Link Control (HDLC), PPP, and tunnel interfaces can be unnumbered.
- 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).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a POS interface, you should configure the POS interface as unnumbered. This strategy allows you to conform to RFC 1195, which states that IP addresses are not required on each interface.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

In the following example, POS interface 0/1/1/0 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 POS 0/1/1/0
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** command in 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 arguments or keywords.

Defaults

IPv4 ICMP unreachables messages are generated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Examples

The following example shows how to disable the generation of ICMP unreachable messages on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
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 global configuration mode. To remove an IPv4 virtual address from the configuration, use the **no** form of this command.

ipv4 virtual address *ipv4-address*/*mask*

no ipv4 virtual address [*ipv4-address*/*mask*]

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. A slash between numbers is required as part of the notation.

Defaults

No IPv4 virtual address is defined for the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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. On a Cisco XR 12000 Series Router in which each RP has multiple Management Ethernet interfaces (two on PRP-1 or three on PRP-2), the virtual IPv4 address maps to whichever Management Ethernet interface on the active RP with which it shares a common IP subnet.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

Examples

The following example shows how to define an IPv4 virtual address:

```
RP/0/RP0/CPU0:router(config)# ipv4 virtual address 10.3.32.154/8
```

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**]

no ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]

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.

Defaults

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example assigns IPv6 address 2001:0DB8:0:1::/64 to POS interface 0/1/1/0 and specifies an EUI-64 interface ID in the low-order 64 bits of the address:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address* **link-local**

no ipv6 address *ipv6-address* **link-local**

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.

Defaults

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 POS interface 0/1/1/0:

```
RP/0/33/1:router(config)# interface POS 0/1/1/0
RP/0/33/1:router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv6 conflict-policy** command in global configuration 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.

Defaults

Default is the lowest rack/slot if no conflict policy is configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 interface 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

This command has no arguments or keywords.

Defaults

IPv6 is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to enable IPv6 processing on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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 global configuration 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.

Defaults

hops: 64 hops

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 global configuration 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.

Defaults

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

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv6 icmp error-interval** command in global configuration 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
```

Related Commands

Command	Description
show ipv6 neighbors	Displays IPv6 neighbors discovery cache information.

ipv6 mtu

To set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface, use the **ipv6 mtu** command in interface 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.

Defaults

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

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

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

Examples

The following example shows how to set the maximum IPv6 packet size for POS interface 0/1/1/0 to 1350 bytes:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 mtu 1350
```

Related Commands

Command	Description
show ipv6 interface	Displays the MTU status of interfaces configured for IPv4.

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 interface 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.

Defaults

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

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

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 POS0
```

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).

Duplicate address detection is performed on all multicast-enabled IPv6 interfaces, including the following interface types:

- Cisco High-Level Data Link Control (HDLC)
- Ethernet, FastEthernet, and GigabitEthernet
- PPP

Task ID

Task ID	Operations
ipv6	read

Examples

The following example 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 POS 0/2/0/1
RP/0/RP1/CPU0:CRS-8_P1(config-if)# ipv6 nd dad attempts 1
```

```
RP/0/RP1/CPU0:CRS-8_P1(config-if)# Uncommitted changes found, commit them before
exiting(yes/no/cancel)? [cancel]:y

RP/0/RP0/CPU0:router# show ipv6 interface

POS0/2/0/0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
POS0/2/0/1 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.
POS0/2/0/2 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.
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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 interface 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 arguments or keywords.

Defaults

The managed address configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to configure the managed address configuration flag in IPv6 router advertisements on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface 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.

Defaults

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

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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 interface 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 arguments or keywords.

Defaults

The other stateful configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example configures the "other stateful configuration" flag in IPv6 router advertisements on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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-advertise** keyword.

ipv6 nd prefix {**ipv6prefix/prefix length | default** [**valid life | at | infinite | no-adv | no-autoconfig | off-link**]}

no ipv6 nd prefix {**ipv6prefix prefix length | default** [**valid life | 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	Specifies all prefixes.
valid-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid.
at	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	The valid lifetime does not expire.
no-ad	The prefix is not advertised.
no-autoconfig	Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	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.

Defaults

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 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Default Parameters

The default keyword can be used to set default parameters for all prefixes.

Prefix Lifetime and Expiration

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.

Onlink

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.

Auto Configuration

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 POS 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 POS 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.
show ipv6 interface	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 interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval *seconds*

no ipv6 nd ra-interval

Syntax Description

seconds	The interval (in seconds) between IPv6 router advertisement transmissions.

Defaults

seconds: 200 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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 interface 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.

Defaults

seconds: 1800 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	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 interface 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.

Defaults

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

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to configure an IPv6 reachable time of 1,700,000 milliseconds for POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

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 arguments or keywords.

Defaults

The default value is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to redirect IPv6 nd-directed broadcasts on POS interface 0/2/0/2:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 nd redirects
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface 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 arguments or keywords.

Defaults

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

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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).

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

Examples

The following example shows how to suppress IPv6 router advertisements on POS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration 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 (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.
hardware-address	The local data-link address (a 48-bit address).

Defaults

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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/RP0/CPU0/0:

```
RP/0/RP0/CPU0:router(config)# ipv6 neighbor 2001:0DB8::45A mgmtEth 0/RP0/CPU0/0
0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbors discovery cache, except static entries.
ipv6 enable	Disables IPv6 processing on an interface that has not been configured with an explicit IPv6 address
show ipv6 neighbors	Displays IPv6 neighbors discovery cache information.

ipv6 unreachables disable

To disable the generation of IPv6 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv6 unreachables disable** command in interface 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 arguments or keywords.

Defaults

IPv6 ICMP unreachables messages are generated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
ipv6	read, write
network	read, write

Examples

The following example shows how to disable the generation of ICMP unreachable messages on POS interface 0/6/0/0:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/6/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 unreachables disable
```

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 global configuration 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.

Defaults

Special default pool if VRF is not specified. By default, this functionality is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

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.

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
local pool ipv4 pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
no local pool ipv4 default
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:

```
local pool ipv4 default 10.1.1.0 10.1.9.255
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:

```
local pool vrf grp1 ipv4 p1_g1 10.1.1.1 10.1.1.50
local pool vrf grp1 ipv4 p2_g1 10.1.1.100 10.1.1.110
local pool vrf grp2 ipv4 p1_g2 10.1.1.1 10.1.1.40
local pool ipv4 lp1 10.1.1.1 10.1.1.10
local pool vrf grp1 ipv4 p3_g1 10.1.2.1 10.1.2.30
local pool vrf grp2 ipv4 p2_g2 10.1.1.50 10.1.1.70
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:

```
local pool vrf vpn1 ipv4 p1_vpn1 10.1.1.1 10.1.1.50
local pool vrf vpn1 ipv4 p2_vpn1 10.1.1.100 10.1.1.110
local pool vrf vpn2 ipv4 p1_vpn2 10.1.1.1 10.1.1.40
local pool ipv4 lp1 10.1.1.1 10.1.1.10
local pool vrf vpn1 ipv4 p3_vpn1 10.1.2.1 10.1.2.30
local pool vrf vpn2 ipv4 p2_vpn2 10.1.1.50 10.1.1.70 group vpn2
local pool ipv4 lp2 10.1.2.1 10.1.2.10
```

These examples show configuration of pools in two vrfs and 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.

Related Commands

Command	Description
show local pool	Displays IPv4 local pool details.

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 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Table 65 describes the significant fields shown in the display.

Table 65 show arm conflicts Command Field Descriptions

Field	Description
F 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 database

To display IPv4 or IPv6 address information stored in the Address Repository Manager (ARM) database, use the **show arm database** command in EXEC mode.

show arm {**ipv4** | **ipv6**} [**vrf** {*vrf-name*}] **database** [**interface** *type instance* | **network** *prefix/length*]

Syntax Description

ipv4	Displays IPv4 address information.
ipv6	Displays IPv6 address information.
vrf	Displays VPN routing and forwarding (VRF) instance information.
vrf-name	
interface	Displays the IPv4 or IPv6 address configured on the specified interface.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
network	Displays addresses that match a prefix.
prefix/length	Network prefix and mask. A slash (/) must precede the specified mask.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

P = Primary, S = Secondary address
|U = Unnumbered
|| Address            Interface                      Producer
P  10.1.1.1/24         Loopback1                       ipv4_io 0/0/0

| Address            Interface  Producer
P 10.4.1.4/24         POS 10/0  ipv4_io 1 10
S 10.4.2.4/24         POS 10/0  ipv4_io 1 10
S 10.4.3.4/24         POS 10/1  ipv4_io 1 10

P = Primary, S = Secondary address

|U = Unnumbered

|| Address            Interface                      Producer
VRF: default
P  12.25.12.10/16     MgmtEth0/RP1/CPU0/0            ipv4_ma 0/RP1/CPU0
```

Table 66 describes the significant fields shown in the display.

Table 66 show arm database Command Field Descriptions

Field	Description
Primary	Primary IP address.
Secondary	Secondary IP address.

Table 66 show arm database Command Field Descriptions (continued)

Field	Description
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 EXEC mode.

show arm [**ipv4**] **router-ids**

Syntax Description

ipv4	(Optional) Displays IPv4 router information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	The **ipv6** and **vrf** keywords were removed.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Table 67 describes the significant fields shown in the display.

Table 67 show arm router-ids Command Field Descriptions

Field	Description
Router-ID	Router identification.
Interface	Interface identification.

show arm registrations producers

To display producer registration information for the Address Repository Manager (ARM), use the **show arm registrations producers** command in EXEC mode.

show arm {ipv4 | ipv6} registrations producers

Syntax Description

ipv4	Displays IPv4 producer registration information.
ipv6	Displays IPv6 producer registration information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 registrations producers** command:

```
RP/0/RP0/CPU0:router# 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
```

Table 68 describes the significant fields shown in the display.

Table 68 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.
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 summary

To display producer registration information for the IP Address Repository Manager (ARM), use the **show arm summary** command in EXEC mode.

show arm {**ipv4** | **ipv6**} **summary**

Syntax Description

ipv4	Displays IPv4 producer registration information.
ipv6	Displays IPv6 producer registration information.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show arm ipv4 summary

IPv4 Producers                          :    5
IPv4 Router id consumers                :    7
IPv4 address conflicts                  :    2
IPv4 unnumbered interface conflicts     :    1
```

Table 69 describes the significant fields shown in the display.

Table 69 show arm summary Command Field Descriptions

Field	Description
IPv4 Producers	Number of IPv4 producers on the router.
IPv4 Router id consumers	Number of IPv4 router ID consumers 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.

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 EXEC mode.

show arm vrf-summary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Table 70 describes the significant fields shown in the display.

Table 70 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 EXEC mode.

show clns statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Table 71 describes the significant fields shown in the display.

Table 71 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 ipv4 interface

To display the usability status of interfaces configured for IPv4, use the **show ipv4 interface** command in EXEC mode.

show ipv4 [**vrf** *vrf-name*] **interface** [*type instance* | **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.
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 (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.
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.

Defaults

If VRF is not specified, the software displays the default VRF.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

```
RP/0/RP0/CPU0:router# show ipv4 interface

Loopback0 is Up, line protocol is Up
  Internet address is 1.0.0.1/8
  Secondary address 10.0.0.1/8
  MTU is 1514 (1514 is available to IP)
  Multicast reserved groups joined: 10.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
POS0/0/0/0 is Up, line protocol is Up
  Internet address is 10.25.58.1/16
  MTU is 1514 (1500 is available to IP)
  Multicast reserved groups joined: 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
POS0/0/0/0 is Shutdown, line protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet protocol processing disabled
```

Table 72 describes the significant fields shown in the display.

Table 72 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[1] 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[2] is enabled or disabled on an interface.
ICMP redirects	Specifies whether ICMPv4[3] 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.

1. MTU = maximum transmission unit
2. ARP = address resolution protocol
3. ICMPv4 = internet control message protocol version 4

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

show local pool

To display IPv4 local pool details, use the **show local pool** command in 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.

Defaults

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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            Free    InUse
P1      172.30.228.11  172.30.228.16  6       0
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
```

Table 73 describes the significant fields shown in the display.

Table 73 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.

Related Commands

Command	Description
local pool	Creates one or more local address pools from which IP addresses are assigned when a peer connects.

show ipv4 traffic

To display statistics about IPv4 traffic, use the **show ipv4 traffic** command in EXEC mode.

show ipv4 traffic [**brief**]

Syntax Description

brief	(Optional) Displays only IPv4 and Internet Control Message Protocol version 4 (ICMPv4) traffic.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	Sample output was modified to display sanity address check drop counters.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

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

```
RP/0/RP0/CPU0:router# show ipv4 traffic

IP statistics:
  Rcvd:  16372 total, 16372 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
         0 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, 0 alert, 0 cipso
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragment count
  Bcast: 0 sent, 0 received
  Mcast: 0 sent, 0 received
   Drop: 0 encapsulation failed, 0 no route, 0 too big, 0 sanity address check
   Sent: 16372 total

ICMP statistics:
  Sent: 0 admin unreachable, 0 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        5 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        5 total
  Rcvd: 0 admin unreachable, 0 network unreachable
        2 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 5 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
        7 total, 0 checksum errors, 0 unknown

UDP statistics:
        16365 packets input, 16367 packets output
        0 checksum errors, 0 no port
        0 forwarded broadcasts

TCP statistics:
        0 packets input, 0 packets output
        0 checksum errors, 0 no port
```

Table 74 describes the significant fields shown in the display.

Table 74 show ipv4 traffic Command Field Descriptions

Field	Description
bad hop count	Occurs when a packet is discarded because its TTL[1] 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.

1. TTL = time-to-live

Related Commands

Command	Description
show ipv6 traffic	Displays statistics about IPv6 traffic.

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in EXEC mode.

show ipv6 [**vrf** *vrf-name*] **interface** [*type instance* | **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.
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 (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.
brief	(Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **summary** keyword was added to the command.
Release 3.4.0	No modification.
Release 3.5.0	The following modifications are listed for the **show ipv6 interface** command: • The command syntax was modified to be similar to the **show ipv4 interface** command. • The sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show ipv6 interface** command provides output similar to the **show ipv4 interface** command, except that it is IPv6-specific.

Task ID

Task ID	Operations
ipv6	read

Examples

The following is sample output from the **show ipv6 interface** command:

```
RP/0/RP0/CPU0:router# show ipv6 interface

GigabitEthernet0/2/0/0 is Up, line protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::212:daff:fe62:c150
  Global unicast address(es):
    202::1, subnet is 202::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ff62:c150 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 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.
  Outgoing access list is not set
  Inbound  access list is not set
```

Table 75 describes the significant fields shown in the display.

Table 75 show ipv6 interface Command Field Descriptions

Field	Description
POS0/3/0/0 is Shutdown, line protocol 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.
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.

Related Commands

Command	Description
show ipv4 interface	Displays the usability status of interfaces configured for IPv4.

show ipv6 neighbors

To display IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in EXEC mode.

show ipv6 neighbors [*interface-type interface-instance* | **location** *node-id*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
location *node-id*	(Optional) Designates a node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

All IPv6 neighbor discovery cache information is displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The following is sample output from the **show ipv6 neighbors** command when entered with an interface type and number:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors POS 0/0/0/0

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH POS2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH POS2
3001:1::45a                                 - 0002.7d1a.9472  REACH POS2
```

The following is sample output from the **show ipv6 neighbors** command when entered with an IPv6 address:

```
RP/0/RP0/CPU0:router# show ipv6 neighbors 2000:0:0:4::2

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH POS2
```

Table 76 describes the significant fields shown in the display.

Table 76 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.

Table 76 show ipv6 neighbors Command Field Descriptions (continued)

Field	Description
State	The state of the neighbor cache entry. Following 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. • ????—Unknown state. Following are the possible states for static entries in the IPv6 neighbor discovery cache: • INCMP (incomplete)—The interface for this entry is down. • reach (reachable)—The interface for this entry is up. **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 was reachable.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show traffic** command in EXEC mode.

show ipv6 traffic [**brief**]

Syntax Description

brief	(Optional) Displays only IPv6 and Internet Control Message Protocol version 6 (ICMPv6) traffic statistics.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	Sample output was modified to display drop counters from the sanity address check.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The following is sample output from 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
```

Table 77 describes the significant fields shown in the display.

Table 77 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.

Table 77 show ipv6 traffic Command Field Descriptions (continued)

Field	Description
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.
ICMP statistics:	Internet Control Message Protocol statistics.

Related Commands

Command	Description
show ipv4 traffic	Displays statistics about IPv4 traffic.

Prefix List Commands on Cisco IOS XR Software

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

For detailed information about prefix list concepts, configuration tasks, and examples, refer to the *Implementing Access Lists and Prefix Lists on Cisco IOS XR Software* configuration module.

clear prefix-list ipv4

To reset the hit count on an IP Version 4 (IPv4) prefix list, use the **clear prefix-list ipv4** command in EXEC mode.

clear prefix-list ipv4 *name* [*sequence-number*]

Syntax Description

name	Name of the prefix list from which the hit count is to be cleared.
sequence-number	(Optional) Sequence number of a prefix list. Range is 1 to 2147483646.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **clear ipv4 prefix-list** to **clear prefix-list ipv4**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The hit count is a value indicating the number of matches to a specific prefix list entry. Use the **clear prefix-list ipv4** command to clear counters for a specified configured prefix list.

Use the *sequence-number* argument to clear counters for a prefix list with a specific sequence number.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example displays IPv4 prefix lists, shows how to clear the counters for list3, then shows how to display the IPv4 prefix lists again, showing that counters are cleared for list3:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.18.30.154/16 (8 matches)
ipv4 prefix-list list2
 20 deny 172.24.30.164/16 (12 matches)
ipv4 prefix-list list3
 30 permit 172.19.31.154/16 (32 matches)

RP/0/RP0/CPU0:router# clear prefix-list ipv4 list3

RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.18.30.154/16 (8 matches)
ipv4 prefix-list list2
 20 deny 172.24.30.164/16 (12 matches)
ipv4 prefix-list list3
 30 permit 172.19.31.154/16
```

Related Commands

Command	Description
deny (prefix-list)	Sets deny conditions for an IPv4 or IP IPv6 prefix list.
ipv4 prefix-list	Defines an IPv4 prefix list.
permit (prefix-list)	Sets permit conditions for an IPv4 or IPv6 prefix list.
show prefix-list ipv4	Displays the configuration of the current IPv4 prefix list.

clear prefix-list ipv6

To reset the hit count on an IP Version 6 (IPv6) prefix list, use the **clear prefix-list ipv6** command in EXEC mode.

clear prefix-list ipv6 *name* [*sequence-number*]

Syntax Description

name	Name of the prefix list from which the hit count is to be cleared.
sequence-number	(Optional) Clears counters for a prefix list with a specific sequence number. Range is 1 to 2147483646.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **clear ipv6 prefix-list** to **clear prefix-list ipv6**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The hit count is a value indicating the number of matches to a specific prefix list entry. Use the **clear prefix-list ipv6** command to clear counters for a specified configured prefix list.

Use the *sequence-number* argument to clear counters for a prefix list with a specific sequence number.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows IPv6 prefix lists, clears the counters for sequence number 60 on prefix list list3, then displays the IPv6 prefix lists again, showing that counters are cleared for sequence number 60:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64 (5 matches)
 60 deny 3000:1::/64 (7 matches)

RP/0/RP0/CPU0:router# clear prefix-list ipv6 list1 60
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64 (5 matches)
 60 deny 3000:1::/64
```

Related Commands

Command	Description
deny (prefix-list)	Sets deny conditions for an IPv4 or IPv6 prefix list.
ipv6 prefix-list	Defines an IPv6 prefix list.
permit (prefix-list)	Sets permit conditions for an IPv4 or IPv6 prefix list.
show prefix-list ipv6	Displays the contents of the current IPv6 prefix list.

copy prefix-list ipv4

To create a copy of an existing IP Version 4 (IPv4) prefix list, use the **copy prefix-list ipv4** command in EXEC mode.

copy prefix-list ipv4 *source-name destination-name*

Syntax Description

source-name	Name of the prefix list to be copied.
destination-name	Destination prefix list where the contents of the *source-name* will be copied.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **copy ipv4 prefix-list** to **copy prefix-list ipv4**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

The following example displays IPv4 prefix lists, shows how to copy prefix-list1 to list4, then displays the IPv4 prefix lists again, showing prefix list4:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.24.20.164/16
ipv4 prefix-list list2
 20 deny 172.18.30.154/16
ipv4 prefix-list list3
 30 permit 172.29.30.154/16

RP/0/RP0/CPU0:router# copy prefix-list ipv4 list1 list4

RP/0/RP0/CPU0:router# show prefix-list ipv4
ipv4 prefix-list list1
 10 permit 172.24.20.164/16
ipv4 prefix-list list2
 20 deny 172.18.30.154/16
ipv4 prefix-list list3
 30 permit 172.29.30.154/16
ipv4 prefix-list list4
 10 permit 172.24.20.164/16
```

Related Commands

Command	Description
ipv4 prefix-list	Defines an IPv4 prefix list.
show prefix-list ipv4	Displays the contents of the current IPv4 prefix lists.

copy prefix-list ipv6

To create a copy of an existing IP Version 6(IPv6) prefix list, use the **copy prefix-list ipv6** command in EXEC mode.

copy prefix-list ipv6 *source-name destination-name*

Syntax Description

source-name	Name of the prefix list to be copied.
destination-name	Destination prefix list where the contents of the *source-name* will be copied.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **copy ipv6 prefix-list** to **copy prefix-list ipv6**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

The following example shows IPv6 prefix lists, shows how to copy prefix-list1 to list4, then displays the IPv6 prefix lists again, showing prefix list4:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
ipv6 prefix-list list2
 10 permit 5555::/24

RP/0/RP0/CPU0:router# copy prefix-list ipv6 list1 list3

RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
ipv6 prefix-list list2
 10 permit 5555::/24
ipv6 prefix-list list3
 40 permit 2000:1::/64
 60 deny 3000:1::/64
```

Related Commands

Command	Description
ipv6 prefix-list	Defines an IPv6 prefix list.
show prefix-list ipv6	Displays the contents of current IPv6 prefix list.

deny (prefix-list)

To set deny conditions for an IP Version 4 (IPv4) or IP Version 6 (IPv6) prefix list, use the **deny** command in IPv4 prefix list configuration or IPv6 prefix list configuration modes. To remove a condition from a prefix list, use the **no** form of this command.

[*sequence-number***] deny** *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]

no *sequence-number* **deny**

Syntax Description

sequence-number	(Optional) Sets deny conditions for a prefix list with a specific sequence number. If you do not use a sequence number, the condition defaults to the next available sequence number in the prefix list. Range is 1 to 2147483646. By default, the first statement is number 10, and the subsequent statements are incremented by 10. The **sequence-number** argument must be used with the **no** form of the command.
network/length	Network number and length (in bits) of the network mask.
ge *value*	(Optional) Specifies a prefix length greater than or equal to the value. It is the lowest value of a range of the *length* (the "from" portion of the length range).
le *value*	(Optional) Specifies a prefix length less than or equal to the value. It is the highest value of a range of the *length* (the "to" portion of the length range).
eq *value*	(Optional) Exact value of the *length*.

Defaults

There is no specific condition under which a packet is denied passing the IPv4 or IPv6 prefix list.

Command Modes

IPv4 prefix list configuration
IPv6 prefix list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The syntax for the **show prefix-list ipv6** command was updated in the examples.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **deny** command to specify conditions under which a packet cannot pass the prefix list.

The **ge**, **le** and **eq** keywords can be used to specify the range of the prefix length to be matched, for prefixes that are more specific than the *network/length* argument. Exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from the **ge** *value* to 32 if only the **ge** keyword is specified. The range is assumed to be from the *length* to the **le** *value argument* if only the **le** attribute is specified.

A specified **ge** *value* or **le** *value* must satisfy the following condition:

length < **ge** *value* < **le** *value* <= 32 (for IPv4)

length < **ge** *value* < **le** *value* <= 128 (for IPv6)

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to deny the route 10.0.0.0/0:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 50 deny 10.0.0.0/0
```

The following example shows how to deny all routes with a prefix of 10.3.32.154:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 80 deny 10.3.32.154 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits routes with a prefix of 172.18.30.154/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 100 deny 172.18.30.154/16 ge 25
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list2
RP/0/RP0/CPU0:router(config-ipv6_pfx)# 70 deny 2000:1::/64 ge 25
```

The following example shows how to add deny conditions to list3, then use the **no** form of the command to remove the condition with the sequence number 30:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3

RP/0/RP0/CPU0:router(config-ipv6_pfx)# deny 2000:1::/64 ge 25
RP/0/RP0/CPU0:router(config-ipv6_pfx)# deny 3000:1::/64 le 32
RP/0/RP0/CPU0:router(config-ipv6_pfx)# deny 4000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y

RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
 30 deny 4000:1::/64 ge 25
```

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RP0/CPU0:router(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
```

Related Commands

Command	Description
permit (prefix-list)	Sets the permit conditions for an IPv4 or IPv6 prefix list.
remark (prefix-list)	Inserts a helpful remark about a prefix list entry.
ipv4 prefix-list	Defines an IPv4 prefix list.
ipv6 prefix-list	Defines an IPv6 prefix list.
show prefix-list ipv4	Displays the contents of the current IPv4 prefix list.
show prefix-list ipv6	Displays the contents of the current IPv6 prefix list.

ipv4 prefix-list

To define an IP Version (IPv4) prefix list by name, use the **ipv4 prefix-list** command in global configuration mode. To remove the prefix list, use the **no** form of this command.

ipv4 prefix-list *name*

no ipv4 prefix-list *name*

Syntax Description

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

Defaults

No IPv4 prefix list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Use the **resequence prefix-list ipv4** command to renumber existing statements and increment subsequent statements to allow a new IPv4 prefix list statement (**permit**, **deny**, or **remark**) to be added. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software will renumber the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write
ipv4	read, write

Examples

The following example shows the prefix lists, then configures list2, then shows the conditions in both prefix lists:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list2

RP/0/RP0/CPU0:router(config-ipv4_pfx)#deny 172.18.30.154/16 ge 25
RP/0/RP0/CPU0:router(config-ipv4_pfx)#
Uncommitted changes found, commit them? [yes]: y

RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

Related Commands

Command	Description
deny (prefix-list)	Sets deny conditions for an IPv4 or IPv6 prefix list.
permit (prefix-list)	Sets permit conditions for an IPv4 or IPv6 prefix list.
remark (prefix-list)	Inserts a helpful remark about a prefix list entry.
resequence prefix-list ipv4	Renumbers existing statements and increments subsequent statements.
show prefix-list ipv4	Displays the contents of the current IPv4 prefix list.

ipv6 prefix-list

To define an IP Version (IPv6) prefix list by name, use the **ipv6 prefix-list** command in global configuration mode. To remove the prefix list, use the **no** form of this command.

ipv6 prefix-list *name*

no ipv6 prefix-list *name*

Syntax Description

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

Defaults

No IPv6 prefix list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ipv6 prefix-list** command to configure an IPv6 prefix list. This command places the router in prefix-list configuration mode, where the denied or permitted access conditions must be defined with the **deny** or **permit** command. You must add a condition to create the prefix list. Use the **remark** command to insert a helpful remark about a prefix list entry.

Task ID

Task ID	Operations
acl	read, write
ipv6	read, write

Examples

The following example shows how to create a prefix list named list-1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list-1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# 40 permit 2000:1::/64
```

```
RP/0/RP0/CPU0:router(config-ipv6-pfx)# 60 deny 3000:1::/64
RP/0/RP0/CPU0:router(config-ipv6-pfx)#
Uncommitted changes found, commit them? [yes]: y

RP/0/0/CPU0:Apr  4 02:12:01.142 : config[65699]: %LIBTARCFG-6-COMMIT : Configura
tion committed by user 'UNKNOWN'.   Use 'show commit changes 1000000022' to view
 the changes.
RP/0/0/CPU0:Apr  4 02:12:01.283 : config[65699]: %SYS-5-CONFIG_I : Configured fr
om console by console

RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
RP/0/RP0/CPU0:router#
```

Related Commands

Command	Description
deny (prefix-list)	Sets deny conditions for an IPv4 or IPv6 prefix list.
permit (prefix-list)	Sets permit conditions for an IPv4 or IPv6 prefix list.
remark (prefix-list)	Inserts a helpful remark about a prefix list entry.
show prefix-list ipv6	Displays the contents of the current IPv6 prefix list.

permit (prefix-list)

To set permit conditions for an IP Version 4 (IPv4) or IP Version 6 (IPv6) prefix list, use the **permit** command in IPv4 prefix list configuration or IPv6 prefix list configuration modes. To remove a condition from a prefix list, use the **no** form of this command.

[*sequence-number*] **permit** *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]

no *sequence-number* **permit**

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the prefix list. This number determines the order of the statements in the prefix list. Range is 1 to 2147483646. By default, the first statement is number 10, and the subsequent statements are incremented by 10.
network/length	Network number and length (in bits) of the network mask.
ge *value*	(Optional) Specifies a prefix length greater than or equal to the value. It is the lowest value of a range of the *length* (the "from" portion of the length range).
le *value*	(Optional) Specifies a prefix length less than or equal to the value. It is the highest value of a range of the *length* (the "to" portion of the length range).
eq *value*	(Optional) Exact value of the *length*.

Defaults

No default behavior or value

Command Modes

IPv4 prefix list configuration
IPv6 prefix list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **permit** command to specify conditions under which a packet can pass the prefix list.

The **ge**, **le** and **eq** keywords can be used to specify the range of the prefix length to be matched, for prefixes that are more specific than the *network/length* argument. Exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from the **ge** *value* to 32 if only the **ge** keyword is specified. The range is assumed to be from the *length* to the **le** *value* argument if only the **le** attribute is specified.

A specified **ge** *value* or **le** *value* must satisfy the following condition:

length < **ge** *value* < **le** *value* <= 32 (for IPv4)

length < **ge** *value* < **le** *value* <= 128 (for IPv6)

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to permit the prefix 172.18.0.0/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# permit 172.18.0.0/16
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 172.20.10.171/16:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv4_pfx)# permit 172.20.10.171/16 le 24
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 2000:1::/64 ge 8 le 24
```

The following example shows how to add permit conditions to list3, then remove the condition with the sequence number 30:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 2000:1::/64 ge 25
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 3000:1::/64 le 32
RP/0/RP0/CPU0:router(config-ipv6_pfx)# permit 3000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y
RP/0/RP0/CPU0:router#show ipv6 prefix-list

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
 20 permit 3000:1::/64 le 32
 30 permit 4000:1::/64 ge 25

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RP0/CPU0:router(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
 20 permit 3000:1::/64 le 32

10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
 30 deny 4000:1::/64 ge 25
```

Related Commands

Command	Description
deny (prefix-list)	Sets deny conditions for an IPv4 or IPv6 prefix list.
remark (prefix-list)	Inserts a helpful remark about a prefix list entry.
ipv4 prefix-list	Creates an IPv4 prefix list.
ipv6 prefix-list	Creates an IPv6 prefix list.
show prefix-list ipv4	Displays the contents of current IPv4 prefix lists.
show prefix-list ipv6	Displays the contents of current IPv6 prefix lists.

remark (prefix-list)

To write a helpful comment (remark) for an entry in either an IP Version 4 (IPv4) or IP Version 6 (IPv6) prefix list, use the **remark** command in IPv4 prefix-list configuration or IPv6 prefix-list configuration modes. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the prefix list. This number determines the order of the statements in the prefix list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10).
remark	Comment that describes the entry in the prefix list, up to 255 characters long.

Defaults

The prefix list entries have no remarks.

Command Modes

IPv4 prefix-list configuration
IPv6 prefix-list configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **remark** command to write a helpful comment for an entry in a prefix list. The remark can be up to 255 characters in length; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Use the **resequence prefix-list ipv4** command if you want to add statements to an existing IPv4 prefix list.

Task ID

Task ID	Operations
acl	read, write

Examples

In the following example, a remark is made to explain a prefix list entry:

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list deny-ten
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 10 remark Deny all routes with a prefix of 10/8
RP/0/RP0/CPU0:router(config-ipv4_pfx)# 20 deny 10.0.0.0/8 le 32
RP/0/RP0/CPU0:router(config-ipv4_pfx)# end
```

In the following example, a remark is made to explain usage:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list list1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# 10 remark use from july23 forward
RP/0/RP0/CPU0:router(config-ipv6-pfx)#
Uncommitted changes found, commit them? [yes]: y

RP/0/0/CPU0:Apr  4 02:20:34.851 : config[65700]: %LIBTARCFG-6-COMMIT : Configura
tion committed by user 'UNKNOWN'.   Use 'show commit changes 1000000023' to view
 the changes.
RP/0/0/CPU0:Apr  4 02:20:34.984 : config[65700]: %SYS-5-CONFIG_I : Configured fr
om console by console
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 10 remark use from july23 forward
 40 permit 2000:1::/64
 60 deny 3000:1::/64
```

Related Commands

Command	Description
ipv4 prefix-list	Creates an entry in a prefix list.
resequence prefix-list ipv4	Renumbers existing statements and increments subsequent statements.
show prefix-list ipv4	Displays information about a prefix list or prefix list entries.

resequence prefix-list ipv4

To renumber existing statements and increment subsequent statements to allow a new prefix list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence prefix-list ipv4** command in EXEC mode.

resequence prefix-list ipv4 *name* [*base* [*increment*]]

Syntax Description

name	Name of a prefix list.
base	(Optional) Number of the first statement in the specified prefix list, which determines its order in the prefix list. Maximum value is 2147483646.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483646.

Defaults

base: 10
increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command name was changed from **resequence ipv4 prefix-list** to **resequence prefix-list ipv4**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. When a match or deny occurs, the router does not go through the rest of the prefix list.

By default, the first statement in a prefix list is sequence number 10, and the subsequent statements are incremented by 10.

Use the **resequence prefix-list ipv4** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv4 prefix list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display the sequence number intervals for prefix list list1, resequence list1 from 10 to 30, and displays the resulting sequence numbers:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25

RP/0/RP0/CPU0:router# resequence prefix-list ipv4 list1 10 30

RP/0/0/CPU0:Apr  4 02:29:39.513 : ipv4_acl_action_edm[183]: %LIBTARCFG-6-COMMIT
: Configuration committed by user 'UNKNOWN'.   Use 'show commit changes 10000000
24' to view the changes.

RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 40 permit 172.18.0.0/16
 70 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

Related Commands

Command	Description
deny (prefix-list)	Sets deny conditions for an IPv4 or IPv6 prefix list.
permit (prefix-list)	Sets permit conditions for an IPv4 or IPv6 prefix list.
remark (prefix-list)	Inserts a helpful remark about a prefix list entry.
show prefix-list ipv4	Displays the contents of the current IPv4 prefix list.

resequence prefix-list ipv6

To renumber existing statements and increment subsequent statements to allow a new prefix list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence prefix-list ipv6** command in EXEC mode.

resequence prefix-list ipv6 *name* [*base* [*increment*]]

Syntax Description

name	Name of a prefix list.
base	(Optional) Number of the first statement in the specified prefix list, which determines its order in the prefix list. Maximum value is 2147483644.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644.

Defaults

base: 10

increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list.

By default, the first statement in a prefix list is sequence number 10, and the subsequent statements are incremented by 10.

Use the **resequence prefix-list ipv6** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv6 prefix list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

The following example shows how to display the sequence number intervals for prefix list list1, resequence list1 from 10 to 30, and displays the resulting sequence numbers:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25

RP/0/RP0/CPU0:router# resequence prefix-list ipv4 list1 10 30

RP/0/0/CPU0:Apr  4 02:29:39.513 : ipv4_acl_action_edm[183]: %LIBTARCFG-6-COMMIT
: Configuration committed by user 'UNKNOWN'.   Use 'show commit changes 10000000
24' to view the changes.
```

show prefix-list ipv4

To display the contents of current IP Version 4 (IPv4) prefix list, use the **show prefix-list ipv4** command in EXEC mode.

show prefix-list ipv4 [*list-name*] [*sequence-number*]

Syntax Description

list-name	(Optional) Name of a prefix list.
sequence-number	(Optional) Sequence number of the prefix list entry. Range is 1 to 2147483646.

Defaults

All IPv4 prefix lists are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command syntax was changed from **show ipv4 prefix-list** to **show prefix-list ipv4**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The prefix for the sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Task ID

Task ID	Operations
acl	read

Examples

The following example displays all configured prefix lists:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

The following example uses the *list-name* argument to display the prefix list named list1:

```
RP/0/RP0/CPU0:router# show prefix-list ipv4 list1

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
```

The following example uses the *list-name* and *sequence-number* argument to display a prefix list named list1 with a sequence number of 10:

```
RP/0/RP0/CPU0:router# show ipv4 prefix-list list1 30

ipv4 prefix-list list1
 30 deny 172.24.20.164/16 ge 25
```

Related Commands

Command	Description
clear prefix-list ipv4	Resest the hit count on an IPv4 prefix list.
ipv4 prefix-list	Defines an IPv4 prefix list.
show prefix-list ipv6	Displays the contents of the current IPv6 prefix list.

show prefix-list ipv6

To display the contents of the current IP Version 6 (IPv6) prefix list, use the **show prefix-list ipv6** command in EXEC mode.

show prefix-list ipv6 [*list-name*] [*sequence-number*] [**summary**]

Syntax Description

list-name	(Optional) Name of a prefix list.
sequence-number	(Optional) Sequence number of the prefix list entry. Range is 1 to 2147483646.
summary	(Optional) Displays summary output of prefix list contents.

Defaults

All IPv6 prefix lists are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The command syntax was changed from **show ipv6 prefix-list** to **show prefix-list ipv6**.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show prefix-list ipv6** command to display the contents of all IPv4 prefix lists.

To display the contents of a specific IPv6 prefix list, use the *name* argument. Use the *sequence-number* argument to specify a given prefix list entry. Use the **summary** keyword to display a summary of prefix list contents.

Task ID

Task ID	Operations
acl	read

Examples

The following example shows how to display all configured prefix lists:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 10 permit 5555::/24
 20 deny 3000::/24
 30 permit 2000::/24
ipv6 prefix-list list2
 10 permit 2000::/24
```

The following example uses the *list-name* argument to display the prefix list named list1:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6 list1

ipv6 prefix-list list1
 10 permit 5555::/24
 20 deny 3000::/24
 30 permit 2000::/24
```

The following example uses the *list-name* and *sequence-number* argument to display a prefix list named list1 with a sequence number of 10:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6 list1 10

ipv6 prefix-list abc
 10 permit 5555::/24
```

The following example displays a summary of prefix list contents:

```
RP/0/RP0/CPU0:router# show prefix-list ipv6 summary

Prefix List Summary:
  Total Prefix Lists configured:        2
  Total Prefix List entries configured: 2
```

Related Commands

Command	Description
clear prefix-list ipv6	Resest the hit count on an IPv4 prefix list.
ipv6 prefix-list	Creates an IPv6 prefix list.
copy prefix-list ipv6	Creates a copy of an existing IPv6 prefix list.

Transport Stack Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure and monitor features related to the transport stack (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 *Configuring TCP, UDP, and RAW Transports on Cisco IOS XR Software* configuration module.

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 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*	Clears statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **location** keyword and *node-id* argument became required.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Related Commands

Command	Description
show raw brief	Displays information about active RAW IP sockets.
show raw statistics pcb	Displays statistics for either a single RAW connection or all RAW connections.

clear tcp pcb

To clear TCP protocol control block (PCB) connections, use the **clear tcp pcb** command in 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*	Clears the TCP connection for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **location** keyword and *node-id* argument became required.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

In the following example, the TCP connection at PCB address 60B75E48 is cleared:

```
RP/0/RP0/CPU0:router# clear tcp pcb 60B75E48
```

Related Commands

Command	Description
show tcp brief	Displays the TCP summary table.

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in EXEC mode.

clear tcp statistics {**pcb** {**all** | *pcb-address*} | **summary**} [**location** *node-id*]

Syntax Description

pcb all	(Optional) Clears statistics for all TCP connections.
pcb *pcb-address*	(Optional) Clears statistics for a specific TCP connection.
summary	(Optional) Clears summary statistic for a specific node or connection.
location *node-id*	(Optional) Clears TCP statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The **summary** keyword was added.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear tcp statistics** command to clear TCP statistics. Use the **show tcp statistics** command to display TCP statistics. You might display TCP statistics and then clear them before you start debugging TCP.

The optional **location** keyword and *node-id* argument can be used to clear TCP statistics for a designated node.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear TCP statistics:

```
RP/0/RP0/CPU0:router# clear tcp statistics
```

Related Commands

Command	Description
show tcp statistics	Displays TCP statistics.

clear udp statistics

To clear User Datagram Protocol (UDP) statistics, use the **clear udp statistics** command in EXEC mode.

clear udp statistics {**pcb** {**all** | *pcb-address*} | **summary**} [**location** *node-id*]

Syntax Description

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*	Clears UDP statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear udp statistics** command to clear UDP statistics. Use the **show udp statistics** command to display UDP statistics. You might display UDP statistics and then clear them before you start debugging UDP.

The optional **location** keyword and *node-id* argument can be used to clear UDP statistics for a designated node.

Task ID

Task ID	Operations
transport	execute

Examples

The following example shows how to clear UDP summary statistics:

```
RP/0/RP0/CPU0:router# clear udp statistics summary
```

Related Commands

Command	Description
show udp statistics	Displays UDP statistics.

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 global configuration 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).

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 MgmtEth interface 0/0/CPU0/0 are forwarded to 172.16.0.1. MgmtEth interface 0/0/CPU0/0 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 MgmtEth 0/0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 helper-address 172.16.0.1
```

Related Commands

Command	Description
helper-address	Configures an address to which UDP broadcasts are forwarded.

service tcp-small-servers

To enable small TCP servers such as the ECHO, use the **service tcp-small-servers** command in global configuration 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.

Defaults

TCP small servers are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Related Commands

Command	Description
service udp-small-servers	Enables small UDP servers such as the ECHO.
show cinetd services	Displays the services whose processes are spawned by cinetd.

service udp-small-servers

To enable small User Datagram Protocol (UDP) servers such as the ECHO, use the **service udp-small-servers** command in global configuration 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.

Defaults

UDP small servers are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Related Commands

Command	Description
service tcp-small-servers	Enables small TCP servers such as the ECHO.

show raw brief

To display information about active RAW IP sockets, use the **show raw brief** command in EXEC mode.

show raw brief [**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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **location** keyword and *node-id* argument became required.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Table 78 describes the significant fields shown in the display.

Table 78 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.
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 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The command name was changed from **show raw pcb** to **show raw detail pcb**.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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, VRF: 0x0
 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
```

Table 79 describes the significant fields shown in the display.

Table 79 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 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The command name was changed from **show raw pcb** to **show raw extended-filters**.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 0/0/CPU0

Total Number of matching PCB's in database: 1
JID: 0/0
Family: 2
PCB: 0x0803dd38
L4-proto: 1
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x3ff
LPTS socket options: 0x0020
Packet Type Filters:
    0
    [220 pkts in]
    3
    [0 pkts in]
    4
    [0 pkts in]
```

Table 80 describes the significant fields shown in the display.

Table 80 show raw 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 statistics pcb

To display statistics for a single RAW connection or for all RAW connections, use the **show raw statistics pcb** command in EXEC mode.

show raw statistics pcb {**all** | *pcb-address*} **location** *node-id*

Syntax Description

all	Displays statistics for all RAW connections.
pcb-address	Displays statistics for a specified RAW connection.
location *node-id*	Displays RAW statistics for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **location** keyword and *node-id* argument became required.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **all** keyword 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.

Task ID

Task ID	Operations
transport	read

Examples

In the following example, statistics for a RAW connection with PCB address 0x80553b0 are displayed:

```
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
```

In this example, statistics for all RAW connections are displayed:

```
RP/0/RP0/CPU0:router# show raw statistics pcb all

Statistics for PCB 0x805484c, Vrfid: 0x60000000
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
```

Table 81 describes the significant fields shown in the display.

Table 81 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.

Related Commands

Command	Description
clear raw statistics pcb	Clears statistics for either a single RAW connection or for all RAW connections.
show raw brief	Displays information about active RAW IP sockets.

show tcp brief

To display a summary of the TCP connection table, use the **show tcp brief** command in EXEC mode.

show tcp brief 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp brief** command:

```
RP/0/RP0/CPU0: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
```

Table 82 describes the significant fields shown in the display.

Table 82 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.
State	State of the TCP connection.

Related Commands

Command	Description
clear tcp pcb	Clears the TCP connection.
clear tcp pcb	Displays details of TCP connections.

show tcp detail

To display the details of the TCP connection table, use the **show tcp detail** command in 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp detail pcb all** command:

```
RP/0/RP0/CPU0:router# show tcp detail pcb all

Connection state is LISTEN, I/O status: 0, socket status: 0
PCB 0x8092774, vrfid 0x0
Local host: 0.0.0.0, Local port: 23
Foreign host: 0.0.0.0, Foreign port: 0

Current send queue size: 0 (max 16384)
Current receive queue size: 0 (max 16384)  mis-ordered: 0 bytes
```

```
Timer          Starts    Wakeups         Next(msec)
Retrans             0          0                 0
SendWnd             0          0                 0
TimeWait            0          0                 0
AckHold             0          0                 0
KeepAlive           0          0                 0
PmtuAger            0          0                 0
GiveUp              0          0                 0
Throttle            0          0                 0
iss: 0          snduna: 0          sndnxt: 0
sndmax: 0          sndwnd: 0          sndcwnd: 1073725440
   irs: 0          rcvnxt: 0          rcvwnd: 16384   rcvadv: 0
```

show tcp extended-filters

To display the details of the TCP extended-filters, use the **show tcp extended-filters** command in EXEC mode.

show tcp 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show tcp extended-filters** command for a specific location (0/0/CPU0):

```
RP/0/RP0/CPU0:router# show tcp extended-filters location 0/0/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
LPTS options: 0x00000000
-----------------------------------

-----------------------------------
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
LPTS options: 0x00000000
-----------------------------------

-----------------------------------
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
LPTS options: 0x00000000
-----------------------------------
```

show tcp statistics

To display TCP statistics, use the **show tcp statistics** command in EXEC mode.

show tcp statistics {**pcb** {**all** | *pcb-address*} | **summary**} [**location** *node-id*]

Syntax Description

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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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, vrfid 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
```

Table 83 describes the significant fields shown in the display.

Table 83 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.

Related Commands

Command	Description
clear tcp statistics	Clears TCP statistics.

show udp brief

To display a summary of the User Datagram Protocol (UDP) connection table, use the **show udp brief** command in EXEC mode.

show udp brief 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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        Recv-Q Send-Q  Local Address          Foreign Address
0x8040c4c      0      0  0.0.0.0:7              0.0.0.0:0
0x805a120      0      0  0.0.0.0:9              0.0.0.0:0
0x805a430      0      0  0.0.0.0:19             0.0.0.0:0
0x805a740      0      0  0.0.0.0:67             0.0.0.0:0
0x804fcb0      0      0  0.0.0.0:123            0.0.0.0:0
```

Table 84 describes the significant fields shown in the display.

Table 84 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.

Related Commands

Command	Description
show tcp brief	Displays details of TCP connections.

show udp detail pcb

To display detailed information of the User Datagram Protocol (UDP) connection table, use the **show udp detail pcb** command in 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*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The command name was changed from **show udp pcb** to s**how udp detail pcb**.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp detail pcb all** command:

```
RP/0/RP1/CPU0:router# show udp detail pcb all location 0/3/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
```

Table 85 describes the significant fields shown in the display.

Table 85 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 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
transport	read

Examples

The following is sample output from the **show udp extended-filters** command for a specific location (0/0/CPU0):

```
RP/0/RP0/CPU0:router# show udp extended-filters location 0/0/CPU0

Total Number of matching PCB's in database: 1
-----------------------------------
JID: 248
Family: 2
PCB: 0x48247e94
L4-proto: 17
Lport: 646
Fport: 0
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x0
LPTS options: 0x00000000
-----------------------------------
```

show udp statistics

To display User Datagram Protocol (UDP) statistics, use the **show udp statistics** command in EXEC mode.

show udp statistics {**summary** | **pcb** {*pcb-address* | *all*}} **location** *node-id*

Syntax Description

summary	Displays summary statistics.
pcb *pcb-address*	Displays detailed statistics for each connection.
pcb *all*	Displays detailed statistics for all connections.
location *node-id*	Displays information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The **location** keyword and *node-id* argument became required.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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:

```
RP/0/RP0/CPU0:router# show udp statistics summary

UDP statistics:
Rcvd: 0 Total, 0 drop, 0 no port
      0 checksum error, 0 too short
Sent: 0 Total, 0 error
0 Total forwarding broadcast packets
0 Cloned packets, 0 failed cloningication
```

Table 86 describes the significant fields shown in the display.

Table 86 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.

Related Commands

Command	Description
clear udp statistics	Clears UDP statistics.

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 global configuration 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.

Defaults

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

Global configuration

Command History

Release	Modification
Release 3.2	This command was supported on the Cisco CRS-1 and the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
transport	read, write

Examples

This example shows how to configure the TCP maximum segment size:

```
RP/0/0/CPU0:(config)# tcp mss 1460
RP/0/0/CPU0:(config)# exit

Uncommitted changes found, commit them? [yes]:
RP/0/0/CPU0: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.
RP/0/0/CPU0: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 global configuration 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.

Defaults

Disabled
age-timer default is 10 minutes

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 global configuration mode. To reset the default, use the **no** form of this command.

tcp selective-ack

no tcp selective-ack

Syntax Description

This command has no arguments or keywords.

Defaults

TCP Selective ACK is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Related Commands

Command	Description
tcp timestamp	Measures the round-trip time of a packet.

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 global configuration 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.

Defaults

The default value for the synwait-time is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 180 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 global configuration mode. To reset the default, use the **no** form of this command.

tcp timestamp

no tcp timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

A TCP time stamp is not used.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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
```

Related Commands

Command	Description
tcp selective-ack	Enables the TCP selective acknowledgment feature.

tcp window-size

To alter the TCP window size, use the **tcp window-size** command in global configuration 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.

Defaults

The default value for the window size is 16k.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Note 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 on Cisco IOS XR Software

This document describes the Cisco IOS XR software commands used to configure and monitor the Virtual Router Redundancy Protocol (VRRP).

For detailed information about VRRP concepts, configuration tasks, and examples, see the *Cisco IOS XR IP Addresses and Services Configuration Guide*.

interface (VRRP)

To enable VRRP interface configuration mode, use the **interface** command in VRRP interface configuration mode. To terminate VRRP interface mode, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.

Defaults

VRRP is disabled.

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Release	Modification
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must configure all VRRP configuration commands in VRRP interface configuration mode.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure VRRP and a virtual router 1 on 10-Gigabit Ethernet interface 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 ipv4 10.0.1.20
```

Related Commands

Command	Description
router vrrp	Configures a VRRP redundancy process.

router vrrp

To configure Virtual Router Redundancy Protocol (VRRP), use the **router vrrp** command in VRRP interface configuration mode. To remove the VRRP configuration, use the **no** form of this command.

router vrrp

no router vrrp

Syntax Description

The command has no argument or keywords.

Defaults

VRRP is not configured.

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must configure all VRRP configuration commands in VRRP interface configuration mode.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure a VRRP with virtual router 1 on 10-Gigabit Ethernet interface 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 priority 254
```

Related Commands

Command	Description
interface (VRRP)	Enables VRRP interface configuration mode.

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 EXEC mode.

show vrrp [**interface** *type instance* [*vrid*]] [**brief | detail | statistics** [**all**]]

Syntax Description

interface	(Optional) Displays the status of the virtual router interface.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
vrid	(Optional) Virtual router identifier, which is the number identifying the virtual router for which status is displayed. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If no interface is specified, all virtual routers are displayed.

Task ID

Task ID	Operations
vrrp	read

Examples

The following sample output is from the **show vrrp** command:

```
RP/0/RP0/CPU0: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         10.0.1.20
Te0/3/0/2      7  100   P Init     unknown         10.1.13.0
```

Table 87 describes the significant fields shown in the display.

Table 87 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 master 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:

```
RP/0/RP0/CPU0:router# show vrrp detail

GigabitEthernet0/5/0/0 - vrID 1
  State is Master
    2 state changes, last state change 00:00:28
  Virtual IP address is 4.0.0.100
  Virtual MAC address is 0000.5E00.0101
  Master router is local
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + 156/256)
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
TenGigE0/3/0/0 - vrID 1
  State is Init
    0 state changes, last state change never
  Virtual IP address is 10.0.1.20
  Virtual MAC address is 0000.5E00.0101
  Master router is unknown
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + 156/256)
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
TenGigE0/3/0/2 - vrID 7
  State is Init
    0 state changes, last state change never
  Virtual IP address is 10.1.13.0
  Virtual MAC address is 0000.5E00.0107
  Master router is unknown
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + 156/256)
  Current priority 100
    Configured priority 100, may preempt
      minimum delay 0 secs
TenGigE0/2/0/4 - vrID 2
   State is Master
     16 state changes, last state change 00:04:55
   Virtual IP address is 7.7.7.123
   Virtual MAC address is 0000.5E00.0101
   Master router is local
   Advertise time 1 secs
     Master Down Timer 3.609 (3 x 1 + 156/256)
   Current priority 80
     Configured priority 100, may preempt
       minimum delay 0 secs
  Tracked items: 1/3 up: 20 decrement
                                          Priority
     Interface                 State     Decrement
     POS0/5/0/2                Down             10
     POS0/5/0/1                Down             10
     TenGigE0/3/0/3            Up               10
```

Table 88 describes the significant fields shown in the displays.

Table 88 show vrrp detail Command Field Descriptions

Field	Description
TenGigE0/3/0/0 - vrID 1	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (master or backup).
Virtual IP address is	Virtual IP address for this interface.
Virtual MAC address is	Virtual MAC address for this interface.
Master router is	Location of the master router.
Advertise time	Interval (in seconds) at which the router sends VRRP advertisements when it is the master virtual router. This value is configured with the **vrrp timer** command.
Master Down Timer	Time the backup router waits for the master router advertisements before assuming the role of master 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 interface.
Configured priority	Priority configured on the interface.
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.

The following sample output is from the **show vrrp** command with the **interface** and **detail** keywords for 10-Gigabit Ethernet interface 0/3/0/0:

```
RP/0/RP0/CPU0:router# show vrrp interface gigabitEthernet 0/3/0/0

                     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         10.0.1.20
Te0/3/0/2      7  100   P Init     unknown         10.1.13.0
```

Table 89 describes the significant fields shown in the displays.

Table 89 show vrrp interface 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 master router.
VRouter addr	Virtual router IP address of the virtual router.

Related Commands

Command	Description
vrrp ipv4	Enables VRRP on an interface and specifies the IP address of the virtual router.

vrrp assume-ownership

To configure a VRRP router to assume ownership of the virtual IP address when in the master state, use the **vrrp assume-ownership** command in VRRP interface configuration mode. To restore the default setting, use the **no** form of this command.

vrrp *vrid* **assume-ownership** [**disable**]

no vrrp *vrid* **assume- ownership** [**disable**]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router for which virtual IP address ownership is being configured. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
disable	(Optional) Does not accept VRRP packets.

Defaults

The master router assumes ownership by default and accepts VRRP packets.

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **vrrp assume-ownership** command specifies that the router assumes ownership of the virtual IP address if it is the master router regardless of whether it is the IP address owner, which means that it accepts packets sent to that IP address during verification of network configuration. If the **vrrp assume-ownership** command is enabled, a router that is not the IP address owner, but is the master router for another IP address, accepts and responds to pings and accepts a Telnet to that router. Accepting packets sent to the other IP address is a useful tool during verification of network configuration.

This command is ignored (irrelevant) when the router is the IP address owner (section 6.4.3 of RFC 2338, *Virtual Router Redundancy Protocol)*.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how the configuration disables the **vrrp assume-ownership** command on 10-Gigabit Ethernet interface 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 ipv4 10.0.0.101 secondary
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 assume-ownership disable
```

Related Commands

Command	Description
vrrp ipv4	Enables VRRP on an interface and specifies the IP address of the virtual router.

vrrp delay

To configure the activation delay for a VRRP router, use the **vrrp delay** command in HSRP interface configuration mode. To delete the activation delay, use the **no** form of this command.

vrrp delay {**minimum** *value* **reload** *value*}

no vrrp delay

Syntax Description

minimum *value*	Sets the minimum delay in seconds for every interface up event. Range is 1 to 10000.
reload *value*	Sets the reload delay in seconds for first interface up event. Range is 1 to 10000.

Defaults

minimum *value:* 1
reload *value:* 5

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **vrrp delay** command delays the start of the VRRP finite state machine (FSM) on an interface up event to ensure that the interface is ready to pass traffic. This ensures that there are no mistaken state changes due to loss of hello packets. The minimum delay is applied on all interface up events and the reload delay is applied on the first interface up event.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure a minimum delay of 10 seconds with a reload delay of 100 seconds:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface mgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp delay minimum 10 reload 100
```

Related Commands

Command	Description
show vrrp	Displays VRRP information.

vrrp ipv4

To enable the Virtual Router Redundancy Protocol (VRRP) on an interface and specify the IP address of the virtual router, use the **vrrp ipv4** command in VRRP interface configuration mode. To disable VRRP on the interface and remove the IP address of the virtual router, use the **no** form of this command.

vrrp *vrid* **ipv4** *ip-address* [**secondary**]

no vrrp *vrid* **ipv4** *ip-address* [**secondary**]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router. Range is 1 to 255.
ip-address	IP address of the virtual router.
secondary	(Optional) Indicates additional IP addresses supported by this group.

Defaults

VRRP is not configured on the interface.

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Configure the **vrrp ipv4** command once without the **secondary** keyword to indicate the virtual router IP address. If you want to indicate additional IP addresses supported by the virtual router, include the **secondary** keyword.

Removing the VRRP configuration from the IP address owner and leaving the IP address of the interface active is considered a misconfiguration because this results in duplicate IP addresses on the LAN.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to enable VRRP on 10-Gigabit Ethernet interface 0/3/0/0. The VRRP virtual router identifier is 1, and 10.0.1.20 is the IP address of the virtual router.

```
RP/0/RP0/1:router(config)# router vrrp
RP/0/RP0/1:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/1:router(config-vrrp-if)# vrrp 1 ipv4 10.0.1.20 secondary
RP/0/RP0/1:router(config-vrrp-if)# vrrp 1 assume-ownership disable
```

Related Commands

Command	Description
show vrrp	Displays a summary or detailed status of one or all configured VRRP virtual routers.

vrrp preempt

To configure the router to take over as master router for a Virtual Router Redundancy Protocol (VRRP) virtual router if it has a higher priority than the current master router, use the **vrrp preempt** command in VRRP interface configuration mode. To disable this preemption, use the **no** form of this command.

vrrp *vrid* **preempt** [**delay** *seconds*] [**disable | enable**]

no vrrp *vrid* **preempt** [**delay** *seconds*] [**disable | enable**]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router for which preemption is being configured. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
delay *seconds*	(Optional) Specifies the number of seconds the router delays before issuing an advertisement claiming virtual IP address ownership to be the master router. Range is 1 to 3600 seconds (1 hour).
disable	(Optional) Disables preemption.
enable	(Optional) Enables preemption.

Defaults

VRRP preempt is enabled.

seconds: 0 (no delay)

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, the router being configured with this command takes over as master router for the virtual router if it has a higher priority than the current master router. You can configure a delay, which causes the VRRP router to wait the specified number of seconds before issuing an advertisement claiming virtual IP address ownership to be the master router.

Note The router that is the virtual IP address owner preempts, regardless of the setting of this command.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure the router to preempt the current master router when its priority of 200 is higher than that of the current master router. If the router preempts the current master router, it waits 15 seconds before issuing an advertisement claiming that it is the master router.

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 preempt delay 15
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 priority 200
```

Related Commands

Command	Description
vrrp ipv4	Enables VRRP on an interface and specifies the IP address of the virtual router.
vrrp priority	Sets the priority of the virtual router.

vrrp priority

To set the priority of the virtual router, use the **vrrp priority** command in VRRP interface configuration mode. To remove the priority of the virtual router, use the **no** form of this command.

vrrp *vrid* **priority** *priority*

no vrrp *vrid* **priority** *priority*

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router for which the priority is being configured. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
priority	Priority of the virtual router. Range is 1 to 254.

Defaults

priority: 100

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use the **vrrp priority** command, you must be a member of a user group associated with the vrrp task ID. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use this command to control which router becomes the master router. This command is ignored while the router is the virtual IP address owner.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure the router with a priority of 254:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 priority 254
```

Related Commands

Command	Description
vrrp ipv4	Enables VRRP on an interface and specifies the IP address of the virtual router.
vrrp preempt	Configures the router to take over as master router for a VRRP virtual router if it has a higher priority than the current master router.

vrrp text-authentication

To configure the simple text authentication used for Virtual Router Redundancy Protocol (VRRP) packets received from other routers running VRRP, use the **vrrp text-authentication** command in VRRP interface configuration mode. To disable VRRP authentication, use the **no** form of this command.

vrrp *vrid* **text-authentication** *string*

no vrrp *vrid* **text-authentication** [*string*]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router for which authentication is being configured. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
string	Authentication string (up to eight alphanumeric characters) used to validate incoming VRRP packets.

Defaults

No authentication of VRRP messages occurs.

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When a VRRP packet arrives from another router in the VRRP group, its authentication string is compared to the string configured on the local system. If the strings match, the message is accepted. If they do not match, the packet is discarded.

All routers within the group must be configured with the same authentication string.

Note Plain text authentication is not meant to be used for security. It simply provides a way to prevent a misconfigured router from participating in VRRP.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure an authentication string of x30dn78k:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 text-authentication x30dn78k
```

Related Commands

Command	Description
vrrp ipv4	Enables VRRP on an interface and specifies the IP address of the virtual router.

vrrp timer

To configure the interval between successive advertisements by the master router in a Virtual Router Redundancy Protocol (VRRP) virtual router, use the **vrrp timer** command in VRRP interface configuration mode. To restore the default value, use the **no** form of this command.

vrrp *vrid* **timer** [**msec**] *interval* [**force**]

no vrrp *vrid* **timer** [**msec**] *interval* [**force**]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router for which timing is being configured. The virtual router identifier is configured with the **vrrp ipv4** command. Range is 1 to 255.
msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds. Range is 20 to 3000 milliseconds.
interval	Time interval between successive advertisements by the master router. The unit of the interval is in seconds, unless the **msec** keyword is specified. Range is 1 to 255 seconds.
force	(Optional) Forces the configured value to be used. This keyword is required if milliseconds is specified.

Defaults

interval: 1 second

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
vrrp	read, write

Examples

The following example shows how to configure the master router to send advertisements every 4 seconds:

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 timer 4
```

Related Commands

Command	Description
vrrp ipv4	Enables VRRP on an interface and specifies the IP address of the virtual router.

vrrp track interface

To configure the Virtual Router Redundancy Protocol (VRRP) to track an interface, use the **vrrp track interface** command in VRRP interface configuration mode. To disable the tracking, use the **no** form of this command.

vrrp *vrid* **track interface** *type instance* [*priority-decrement*]

no vrrp *vrid* **track interface** *type instance* [*priority-decrement*]

Syntax Description

vrid	Virtual router identifier, which is the number identifying the virtual router to which tracking applies.
type	Interface type. For more information, use the question mark (**?**) online help function.
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 (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.
priority-decrement	(Optional) Amount by which the priority for the router is decremented (or incremented) when the tracked interface goes down (or comes back up). Decrements can be set to any value between 1 and 254. Default value is 10.

Defaults

The default decrement value is 10. Range is 1 to 254.

Command Modes

VRRP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **vrrp track interface** command ties the priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if IP on that interface is up. Otherwise, the tracked interface is down.

You can configure VRRP to track an interface that can alter the priority level of a virtual router for a VRRP virtual router. When the IP protocol state of an interface goes down or the interface has been removed from the router, the priority of the backup virtual router is decremented by the value specified in the *priority-decrement* argument. When the IP protocol state on the interface returns to the up state, the priority is restored.

Task ID

Task ID	Operations
vrrp	read, write

Examples

In the following example, 10-Gigabit Ethernet interface 0/3/0/0 tracks interface 0/3/0/3 and 0/3/0/2. If one or both of these two interfaces go down, the priority of the router decreases by 10 (default priority decrement) for each interface. The default priority decrement is changed using the *priority-decrement* argument. In this example, because the default priority of the virtual router is 100, the priority becomes 90 when one of the tracked interfaces goes down and the priority becomes 80 when both go down. See the **vrrp priority** command for details on setting the priority of the virtual router.

```
RP/0/RP0/CPU0:router(config)# router vrrp
RP/0/RP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 track interface TenGigE 0/3/0/3
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 track interface TenGigE 0/3/0/2
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 preempt delay 15
RP/0/RP0/CPU0:router(config-vrrp-if)# vrrp 1 ipv4 192.92.72.46
```

Related Commands

Command	Description
vrrp priority	Sets the priority of the virtual router.

INDEX

AR	Cisco IOS XR Advanced System Command Reference
HR	Cisco IOS XR Interface and Hardware Component Command Reference
IR	Cisco IOS XR IP Addresses and Services Command Reference
MCR	Cisco IOS XR Multicast Command Reference
MNR	Cisco IOS XR System Monitoring Command Reference
MPR	Cisco IOS XR MPLS Command Reference
QR	Cisco IOS XR Modular Quality of Service Command Reference
RR	Cisco IOS XR Routing Command Reference
SBR	Cisco IOS XR Session Border Controller Command Reference
SMR	Cisco IOS XR System Management Command Reference
SR	Cisco IOS XR System Security Command Reference

A

C

D

F

H

I

L

P

R

S

T

V