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 clns traffic

To clear Connectionless Network Service (CLNS) traffic statistics, use the **clear clns traffic** command in EXEC mode.

clear clns traffic

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 modifications.
Release 3.2	This command was supported on the 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*.

Examples

The following example shows how to clear CLNS traffic statistics:

```
RP/0/RP0/CPU0:router# clear clns traffic
```

Related Commands

Command	Description
show clns traffic	Displays CLNS traffic statistics.

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 modifications.
Release 3.2	This command was supported on the 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*.

If the location option is specified, only the neighbor entries specified in the location node-id keyword and argument are cleared.

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 frequency 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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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 An 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.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note If any networking device on a network segment uses a secondary IPv4 address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can quickly cause routing loops.

Note When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

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.
longets-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.

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*.

Examples

The following example shows how to enable the static policy for conflict resolution:

```
RP/0/RP0/CPU0:router(config)# ipv4 conflict-policy static
```

ipv4 directed-broadcast

To enable forwarding of IPv4 directed broadcasts on an interface, use the **ipv4 directed-broadcast** command in interface configuration mode. To disable forwarding of IPv4 directed broadcast on an interface, use the **no** form of this command.

ipv4 directed-broadcast

no ipv4 directed-broadcast

Syntax Description

This command has no 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 modifications.
Release 3.2	This command was supported on the 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*.

A directed broadcast is a packet sent to a specific network or a series of networks by default. IPv4 directed broadcasts are dropped and not forwarded. Dropping IPv4 directed broadcasts makes routers less susceptible to denial-of-service (DoS) attacks.

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	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 *destination-address*

no ipv4 helper-address *destination-address*

Syntax Description

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.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

This command enables the Cisco IOS XR software to respond to IPv4 ICMP mask requests by sending ICMP mask reply messages.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

All devices on a physical medium must have the same protocol MTU in order 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.

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
```

ipv4 redirects disable

To disable 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 disable** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipv4 redirects disable

no ipv4 redirects disable

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 modifications.
Release 3.2	This command was supported on the 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*.

If HSRP is configured on an interface, ICMP redirect messages are disabled by default on that interface.

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 disable
```

ipv4 source-route disable

To disable the handling of IPv4 datagrams with source routing header options, use the **ipv4 source-route** command in global configuration mode. To have the software discard any IPv4 datagrams containing a disable source route option, use the **no** form of this command.

ipv4 source-route disable

no ipv4 source-route disable

Syntax Description

This command has no arguments or keywords.

Defaults

The software discards any IPv4 datagrams containing a source router option, unless Hot Standby Router Protocol (HSRP) 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 modifications.
Release 3.2	This command was supported on the 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*.

Examples

The following example shows how to disable the handling of IP datagrams with source routing header options:

```
RP/0/RP0/CPU0:router(config)# ipv4 source-route disable
```

ipv4 unnumbered

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: • 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 will vary 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 modifications.
Release 3.2	This command was supported on the 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*.

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 with RFC 1195, which states that IP addresses are not required on each interface.

Note Using an unnumbered Packet-over-SONET (PoS) interface between different major networks (or *majornets*) requires caution. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, then any routing protocol running across the PoS interface must not advertise subnet information.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 interface, 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 mark between numbers is required as part of the notation.

Defaults

No IPv4 virtual address is defined for the interface.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modifications.
Release 3.2	This command was supported on the 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*.

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.

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
```

Note Using an unnumbered Packet-over-SONET (PoS) interface between different major networks (or *majornets*) requires caution. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, then any routing protocol running across the PoS interface must not advertise subnet information.

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 virtual address 192.168.6.6 255.255.255.0
RP/0/RP0/CPU0:router# interface POS 0/1/1/0
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5
```

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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. 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, 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.

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.
longets-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.

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*.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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. Default is 100 milliseconds.
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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

All devices on a physical medium must have the same protocol MTU in order 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.

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
```

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. Default is 1 message.

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 modifications.
Release 3.2	This command was supported on the 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*.

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

Examples

The following examples display the state (tentative or duplicate) of the unicast IPv6 address configured for an interface:

```
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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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. The default is 200 seconds.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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. The default is 1800 seconds.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 modifications.
Release 3.2	This command was supported on the 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*.

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 scavenge-timeout

To set the lifetime for stale neighbor entries, use the **ipv6 nd scavenge-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd scavenge-timeout *seconds*

no ipv6 nd scavenge-timeout

Syntax Description

seconds	Range is 0 to 43200 seconds. Default is 12 hours (43200 seconds).

Defaults

seconds: 43200 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 modifications.
Release 3.2	This command was supported on the 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*.

This command is used to set the lifetime for neighbor entries in the stale state. When the scavenge-timer for a neighbor entry expires, the entry is cleared.

Examples

The following example shows how to set the scavenge-timeout to 9000 seconds 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 scavenge-timeout 9000
```

Related Commands

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.
show ipv6 neighbors	Display IPv6 neighbor discovery cache information.

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 modifications.
Release 3.2	This command was supported on the 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*.

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).

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 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: • 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 will vary 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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 PoS interface 0/1/1/0:

```
RP/0/RP0/CPU0:router(config)# ipv6 neighbor 2001:0DB8::45A POS 0/1/1/0 0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbors discovery cache, except static entries.
no 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.

mhost ipv4 default-interface

To configure the default interface for IPv4 multicast transmission and reception to and from the host stack, use the **mhost ipv4 default-interface** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

mhost ipv4 default-interface *type instance*

no mhost ipv4 default-interface

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: • 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.

Defaults

The system chooses an arbitrary interface as the mhost default interface.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modifications.
Release 3.2	This command was supported on the 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*.

The **mhost ipv4 default-interface** command configures the interface that the Auto-RP, ping, and mtrace applications use for multicast transmissions, and the interface that multicast groups join for reception. Any other applications that do not specify an interface use this interface for multicast transmissions and reception.

Auto-RP, ping, and mtrace may use the mhost default interface to process multicast messaging. When the **multicast-routing ipv4** command is enabled, packets sent to the mhost default interface are also switched out other interfaces with a matching forwarding state. In addition, an arbitrary interface may be chosen to be the active mhost default interface if the configured interface is not operational. If no mhost default interface is configured with this command, an arbitrary interface is chosen as the active mhost default.

Examples

The following example shows how to configure PoS 2/1/0/1 as the default interface:

```
RP/0/RP0/CPU0:router(config)# mhost ipv4 default-interface POS 2/1/0/1
```

Related Commands

Command	Description
show ipv4 traffic	Displays the configured default interface and active default interface.

router-id (global)

To configure the global router ID for the router, use the **router-id** command in global configuration mode. To remove the global router ID, use the **no** form of this command.

router-id {*interface-type interface-instance* | *router-id*}

no router-id

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: • 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 will vary depending on interface type. For more information about the syntax for the router, use the question mark (**?**) online help function.
router-id	IPv4 address that will be used as the global router ID.

Defaults

No global router ID is set on the router.

Note The routing protocols select router IDs from loopback addresses if no global router ID is configured on the router.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modifications.
Release 3.2	This command was supported on the 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*.

Examples

The following example shows how to set the global router ID to 10.3.32.154:

```
RP/0/RP0/CPU0:router(config)# router-id 10.3.32.154
```

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**} **conflicts** [**address** | **override** | **unnumbered**]

Syntax Description

ipv4	Displays IPv4 address conflicts.
ipv6	Displays IPv6 address conflicts.
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 modifications.
Release 3.2	This command was supported on the 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*.

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.

Examples

The following sample is output 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

tu2->tu1                       tu1->Lo1
```

Table 49 describes the significant fields shown in the display.

Table 49 show arm conflicts 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**} **database** [**interface** *type instance* | **network** *prefix/length*]

Syntax Description

ipv4	Displays IPv4 address information.
ipv6	Displays IPv6 address information.
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: • 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.
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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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
```

Table 50 describes the significant fields shown in the display.

Table 50 show arm database Field Descriptions

Field	Description
Primary	Primary IP address.
Secondary	Secondary IP address.
Unnumbered Address	Interface is unnumbered and the address displayed is that of the referenced interface.
Interface	Interface that has this IP address.
Producer	Process that provides the IP address to the ARM.

show arm registrations consumers routerid

To display router ID consumer registration information for the Address Repository Manager (ARM), use the **show arm registrations consumers routerid** command in EXEC mode.

show arm {ipv4 | ipv6} registrations consumers routerid

Syntax Description

ipv4	Displays IPv4 router ID consumer registration information.
ipv6	Displays IPv6 router ID consumer 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 modifications.
Release 3.2	This command was supported on the 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*.

Use the **show arm registrations consumers routerid** command to display information about clients that register with ARM to obtain router ID information. Registration information is displayed with the consumer ID, the router ID, and the interface type and number.

Examples

The following is sample output from the **show arm ipv4 registrations consumers routerid** command:

```
RP/0/RP0/CPU0:router# show arm ipv4 registrations consumers routerid

G = The router id is the global router id
|O = Only the global router id is requested
||N = The global router id is not requested
||| Consumer Id               Router Id                              Interface

 O  mpls_rid_helper           0.0.0.0                                    None
    BGP                       10.1.1.1                               Loopback1
    fibv4                     10.1.1.1                               Loopback1
    fibv4                     10.1.1.1                               Loopback1
    fibv4                     10.1.1.1                               Loopback1
    fibv4                     10.1.1.1                               Loopback1
```

Table 51 describes the significant fields shown in the display.

Table 51 show arm registrations consumers routerid Field Descriptions

Field	Description
G = The router id is the global router id |O = Only the global router id is requested ||N = The global router id is not requested	Legend defining symbols that may appear in the output for this command.
Consumer Id	Indicates the router ID consumer process.
Router Id	Indicates the router ID used by the consumer.
Interface	Interface type and number associated of the router ID used by the consumer.

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 modifications.
Release 3.2	This command was supported on the 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*.

Use the **show arm registrations producers** command to display information on producers of IP ARM registrations. Registration information is displayed with the ID.

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 52 describes the significant fields shown in the display.

Table 52 show arm registrations producers 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 modifications.
Release 3.2	This command was supported on the 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*.

Use the **show arm summary** command to display a summary of the number of producers, address conflicts, and unnumbered interface conflicts in the router.

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 53 describes the significant fields shown in the display.

Table 53 show arm summary 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 clns traffic

To display Connectionless Network Service (CLNS) protocol statistics, use the **show clns traffic** command in EXEC mode.

show clns traffic

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 modifications.
Release 3.2	This command was supported on the 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*.

Use this command to display CLNS statistics.

Examples

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

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

CLNS Statistics
Last counter clear                    399 seconds ago
Total number of packets sent          99
Total number of packets received      230
Send packets dropped, buffer overflow 123
Send packets dropped, out of memory   0
Send packets dropped, other           0
Receive socket max queue size         1
Class    Overflow/Max   Rate Limit/Max
IIH             123/23              0/0
LSP             0/0                 0/0
SNP             0/0                 0/0
OTHER           0/0                 0/0
Total           0
```

Table 54 describes the significant fields shown in the display.

Table 54 show clns traffic Field Descriptions

Field	Description
Class Overflow/Max Rate Limit/Max	Lists the number of packet drops per packet type and the maximum number of drops in a row.
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.

Related Commands

Command	Description
clear clns traffic	Clears CLNS traffic statistics.

show ipv4 interface

To display the usability status of interfaces configured for IPv4, use the **show ipv4 interface** command in EXEC mode.

show ipv4 interface [*type instance* | **brief** | **summary**]

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: • 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.
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

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 modifications.
Release 3.2	This command was supported on the 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*.

The **show ipv4 interface** command provides output similar to the **show ipv6 interface** command, except that it is IPv4-specific.

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
POS0/2/0/0 is Shutdown, line protocol is Down
  Internet protocol processing disabled
POS0/2/0/1 is Shutdown, line protocol is Down
  Internet protocol processing disabled
POS0/2/0/2 is Shutdown, line protocol is Down
  Internet protocol processing disabled
POS0/2/0/3 is Shutdown, line protocol is Down
  Internet protocol processing disabled
```

Table 55 describes the significant fields shown in the display.

Table 55 show ipv4 interface 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.

Table 55 show ipv4 interface Field Descriptions (continued)

Field	Description
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 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 modifications.
Release 3.2	This command was supported on the 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*.

The **show ipv4 traffic** command provides output similar to the **show ipv6 traffic** command, except that it is IPv4-specific.

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
   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 56 describes the significant fields shown in the display.

Table 56 show ipv4 traffic 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 interface [*type instance* | **brief** | **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: • 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.
brief	(Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
location *node-id*	(Optional) Designates a 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 modifications.
Release 3.2	This command was supported on the 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*.

The **show ipv6 interface** command provides output similar to the **show ipv4 interface** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 interface** command:

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

Loopback0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
POS0/0/CPU0/0 is Up, line protocol is Up
  IPv6 is enabled, link-local address is fe80::203:fdff:fe1b:47fe
  Global unicast address(es):
    1ff:1::2, subnet is 1ff:1::/64
  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
  Hosts use stateless autoconfig for addresses.
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
  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 Up, line protocol is Up
  IPv6 is enabled, link-local address is fe80::200:11ff:fe11:1111
  Global unicast address(es):
    111::2, subnet is 111::/64
  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.
POS0/3/0/0 is Shutdown, line protocol is Down
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
POS0/3/0/1 is Shutdown, line protocol is Down
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
```

```
POS0/3/0/2 is Up, line protocol is Down
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
POS0/3/0/3 is Shutdown, line protocol is Down
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
RP/0/RP0/CPU0:router#
```

Table 57 describes the significant fields shown in the display.

Table 57 show ipv6 interface 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).

Table 57 show ipv6 interface Field Descriptions (continued)

Field	Description
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

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 will vary 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 modifications.
Release 3.2	This command was supported on the 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*.

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.

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 2

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 58 describes the significant fields shown in the displays.

Table 58 show ipv6 neighbors 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 58 show ipv6 neighbors 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 modifications.
Release 3.2	This command was supported on the 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*.

The **show ipv6 traffic** command provides output similar to the **show ipv4 traffic** command, except that it is IPv6-specific.

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
  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:
        0 packets input, 0 checksum errors, 0 dropped
        0 packets output, 0 retransmitted
```

Table 59 describes the significant fields shown in the display.

Table 59 show ipv6 traffic Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
total	Total number of packets received by the software.
local destination	Locally destined packets received by the software.
source-routed	Packets seen by the software with RH.
truncated	Truncated packets seen by the software.
bad header	An error was found in generic HBH, RH, DH, or HA. Software only.
unknown option	Unknown option type in IPv6 header.
unknown protocol	Protocol specified in the IP header of the received packet is unreachable.
Sent:	Statistics in this section refer to packets sent by the router.
forwarded	Packets forwarded by the software. If the packet cannot be forwarded in the first lookup (for example, the packet needs option processing), then the packet is not included in this count, even if it ends up being forwarded by the software.

Table 59 show ipv6 traffic Field Descriptions (continued)

Field	Description
Mcast:	Multicast packets.
ICMP statistics:	Internet Control Message Protocol statistics.

Related Commands

Command	Description
show ipv4 traffic	Displays statistics about IPv4 traffic.

show mhost ipv4 default-interface

To display information about IPv4 multicast host (mhost) interface that is being utilized on the router, use the **show mhost ipv4 default-interface** command in EXEC mode.

show mhost ipv4 default-interface

Syntax Description

This command has no keywords or arguments.

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 modifications.
Release 3.2	This command was supported on the 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*.

The **show mhost ipv4 default-interface** command displays the mhost default address of the configured and currently active default interface.

Examples

The following is sample output from the **show mhost ipv4 default-interface** command. The output is self explanatory.

```
RP/0/RP0/CPU0:router# show mhost ipv4 default-interface

mhost configured default interface is 'Loopback1'
mhost active default interface is 'Loopback1'
```

Related Commands

Command	Description
mhost ipv4 default-interface	Configures the IPv4 mhost default interface.
show mhost ipv4 groups	Displays the IPv4 mhost groups joined on an interface.

show mhost ipv4 groups

To display the IPv4 multicast host (mhost) groups joined on an interface, use the **show mhost ipv4 groups** command in EXEC mode.

show mhost ipv4 groups *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 will vary 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 mhost groups joined on an interface from the designated node. The *node-id* argument is entered in the *rack/slot/module/port* 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 modifications.
Release 3.2	This command was supported on the 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*.

If you do not specify a node with the **location** keyword and *node-id* argument, this command displays the mhost groups joined from the route processor (RP) from which the command had been issued.

Examples

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

```
RP/0/RP0/CPU0:router# show mhost ipv4 groups Loopback 1

Loopback1
  192.168.0.37 :includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  172.16.0.36 :includes 1, excludes 0, mode INCLUDE
    1.1.1.1 :includes 1, excludes 0, active in INCLUDE filter
  192.168.0.35 :includes 0, excludes 1, mode EXCLUDE
    1.1.1.1 :includes 0, excludes 1, active in EXCLUDE filter
```

This command displays the multicast groups joined on the specified interface. It also displays the number of sockets that have set up an include mode or an exclude filter for that group, and if there are any source-specific filters.

For example, for the 192.168.0.37 group one socket is interested in that group in the exclude mode with no source filters, that is, exclude none or include all sources. For the 172.16.0.36 group, one socket is interested in that group in the include mode with one active source filter, that is, the socket is interested in that group from only the 1.1.1.1 source. For the 192.168.0.35 group, there is one socket is interested in that group in the exclude mode with one active source filter, that is, the socket is interested in that group from all sources other than that source, 1.1.1.1.

Related Commands

Command	Description
mhost ipv4 default-interface	Configures the IPv4 mhost default interface.
show mhost ipv4 default-interface	Displays information about the IPv4 mhost default interface.