Network Stack IPv4 and IPv6 Commands

This chapter describes the commands available on 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 *Cisco IOS XR IP Addresses and Services Configuration Guide for the Cisco XR 12000 Series Router*.

- show ipv6 neighbors , page 88
- show ipv6 neighbors summary , page 93
- show ipv6 traffic , page 94
- show mpa client, page 97
- show mpa groups, page 98
- show mpa ipv4, page 100
- show mpa ipv6, page 102
- show svd role, page 104
- show vrf, page 105
- show vrf-group, page 107
- vrf, page 108
- vrf(address-family), page 109
- vrf-group, page 110
- vrf (description), page 111
- vrf (mhost), page 112

clear ipv6 duplicate address

To trigger a Duplicate Address Detection (DAD) request for addresses that are found in DUPLICATE status, use the **clear ipv6 duplicate address** command. If a request is already triggered , then the **clear ipv6 duplicate address** command clears the DUPLICATE status of an address and makes it usable.

clear ipv6 duplicate address [*interface-type interface-path-id*]

Syntax Description

interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

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

If none of the optional keywords is specified, the command iterates through all the duplicate addresses and retriggers a DAD request for each of these addresses.

Task ID

Task ID	Operations
network	read, write
IPv6	execute

The following example shows how to use the **clear ipv6 duplicate address** command:

```
RP/0/0/CPU0:router# clear ipv6 duplicate address
```

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.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
network	read, write
IPv6	execute

In the following example, only the highlighted entry is deleted:

```
RP/0/0/CPU0:router# clear ipv6 neighbors ?
location specify a node name

RP/0/0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH POS0/0/0/0
8888::8 - 1234.2345.9877 REACH POS/0/0/0
fe80::205:1ff:fe9f:6400 1335 0005.019f.6400 STALE POS0/0/0/0
fe80::206:d6ff:fece:3808 1482 0006.d6ce.3808 STALE POS0/0/0/0
fe80::200:11ff:fe11:1112 1533 0000.1111.1112 STALE POS0/2/0/2

RP/0/0/CPU0:router# clear ipv6 neighbors location 0/2/0
RP/0/0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH POS0/0/0/0
8888::8 - 1234.2345.9877 REACH POS0/0/0/0
fe80::205:1ff:fe9f:6400 1387 0005.019f.6400 STALE POS0/0/0/0
fe80::206:d6ff:fece:3808 1534 0006.d6ce.3808 STALE POS0/0/0/0
```

icmp ipv4 rate-limit unreachable

To limit the rate that IPv4 Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **icmp ipv4 rate-limit unreachable** command in global configuration mode. To remove the rate limit, use the **no** form of this command.

icmp ipv4 rate-limit unreachable [DF] *milliseconds*

no icmp ipv4 rate-limit unreachable [DF] *milliseconds*

Syntax Description

DF	(Optional) Limits the rate at which ICMP destination unreachable messages are sent when code 4 fragmentation is needed and data fragmentation is (DF) set, as specified in the IP header of the ICMP destination unreachable message.
milliseconds	Time period (in milliseconds) between the sending of ICMP destination unreachable messages. Range is 1 to 4294967295.

Command Default

The default value is one ICMP destination unreachable message every 500 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

The Cisco IOS XR softwaremaintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **DF** option is not configured, the **icmp ipv4 rate-limit unreachable** command sets the time values for DF destination unreachable messages. If the **DF** option is configured, its time values remain independent from those of general destination unreachable messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to set the time interval for the ICMP destination unreachable message to be generated at a minimum interval of 10 ms:

```
RP/0/0/CPU0:router(config)# icmp ipv4 rate-limit unreachable 10
```

icmp source

To select the appropriate source IP address to be inserted in the ICMP response packets for generating exception packets (ICMP responses to packets that cannot be forwarded), use the **icmp source** command. To discard an IP address inserted in the ICMP response packets, use the **no** form of this command.

icmp ipv4 source {**rfc**| **vrf**}

no icmp ipv4 source {**rfc**| **vrf**}

Syntax Description

ipv4	Specifies an IPv4 address.
ipv6	Specifies an IPv6 address.
rfc	Enables RFC compliance for source address selection.
vrf	Enables VRF source address selection.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.8.0	This command was introduced.

Usage Guidelines

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

The **rfc** keyword selects a source address that conforms to RFC 1812. RFC 1812 states that when generating an ICMP packet, the source address must be one of the addresses on the outgoing physical interface. If such an address is not available, selection may resort to the global router ID.

The **vrf** keyword selects a source address relevant to the VRF, in which the packet is interpreted.

Task ID

Task ID	Operations
network	read, write

The following example shows how to use the **icmp source**command:

```
RP/0/0/CPU0:router(config)#icmp ipv4 source vrf
```

ipv4 address (network)

To set a primary or secondary IPv4 address for an interface, use the **ipv4 address** command in interface configuration mode. To remove an IPv4 address, use the **no** form of this command.

ipv4 address *ipv4-address mask* **[secondary]** [**route-tag** *route-tag value*]

no ipv4 address *ipv4-address mask* **[secondary]** [**route-tag** *route-tag value*]

Syntax Description

ipv4-address	IPv4 address.
mask	Mask for the associated IP subnet. The network mask can be specified in either of two ways: • The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.
secondary	(Optional) Specifies that the configured address is a secondary IPv4 address. If this keyword is omitted, the configured address is the primary IPv4 address.
route-tag	(Optional) Specifies that the configured address has a route tag to be associated with it.
route-tag value	(Optional) Value of the route tag. Range is 1 to 4294967295.

Command Default

No IPv4 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	The **route-tag** keyword was added.

Usage Guidelines

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

An interface can have one primary IPv4 address and multiple secondary IPv4 addresses. Packets generated by the software always use the primary IPv4 address. Therefore, all networking devices on a segment should share the same primary network number.

Note The same IPv4 address configured on two different interfaces causes an error message to display that indicates the conflict. The interface located in the highest rack, slot, module, instance, and port is disabled.

Hosts can determine subnet masks using the IPv4 Internet Control Message Protocol (ICMP) mask request message. Networking devices respond to this request with an ICMP mask reply message.

You can disable IPv4 processing on a particular interface by removing its IPv4 address with the **no ipv4 address** command. If the software detects another host using one of its IPv4 addresses, it will display an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except that the system never generates datagrams other than routing updates with secondary source addresses. IPv4 broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IPv4 addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IPv4 addresses on the networking devices allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.

The route-tag feature attaches a tag to all IPv4 addresses. The tag is propagated from the Management Agents (MA) to the Address Repository Managers (RPM) to routing protocols, thus enabling the user to control the redistribution of connected routes by looking at the route tags via RPL scripts.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

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 interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface gigabitethernet  0/1/1/0
```

```
RP/0/0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0
RP/0/0/CPU0:router(config-if)# ipv4 address 192.168.7.17 255.255.255.0 secondary
RP/0/0/CPU0:router(config-if)# ipv4 address 192.168.8.17 255.255.255.0 secondary
```

Related Commands

Command	Description
show ipv4 interface , on page 72	Lists a summary of IPv4 information and status for the interface.

ipv4 assembler max-packets

To configure the maximum number of packets that are allowed in assembly queues, use the **ipv4 assembler max-packets** command in global configuration mode. To disable this feature, use the **no** from of this command.

ipv4 assembler max-packets *percentage value*

no ipv4 assembler max-packets *percentage value*

Syntax Description

percentage value	Percentage of total packets available in the system. The range is from 1 to 50.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to configure the maximum number of packets for the assembly queue:

```
RP/0/0/CPU0:router(config)# ipv4 assembler max-packets 35
```

Related Commands

Command	Description
ipv4 assembler timeout, on page 11	Configures the number of seconds an assembly queue can hold before a timeout occurs.

ipv4 assembler timeout

To configure the number of seconds an assembly queue can hold before a timeout occurs, use the **ipv4 assembler timeout** command in global configuration mode mode. To disable this feature, use the **no** form of this command.

ipv4 assembler timeout *seconds*

no ipv4 assembler timeout *seconds*

Syntax Description

seconds	Number of seconds an assembly queue can hold before a timeout occurs. The range is from 1 to 120.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to configure an assembly queue before a timeout occurs:

```
RP/0/0/CPU0:router(config)# ipv4 assembler timeout 88
```

Related Commands

Command	Description
ipv4 assembler max-packets, on page 10	Configures the maximum number of packets that are allowed in assembly queues.

ipv4 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv4 conflict-policy** command in global configuration mode mode. To disable the IPARM conflict resolution, use the **no** form of the command.

ipv4 conflict-policy {**highest-ip**| **longest-prefix**| **static**}

no ipv4 conflict-policy {**highest-ip**| **longest-prefix**| **static**}

Syntax Description

highest-ip	Keeps the highest ip address in the conflict set.
longest-prefix	Keeps the longest prefix match in the conflict set.
static	Keeps the existing interface running across new address configurations.

Command Default

The precedence rule adopted is loopback > physical > other virtual interfaces. Within virtual interfaces, there is an alphabetical preference, for example, loopback1 > loopback2 and bundle-ether > bundle-pos > tunnel. Among physical interfaces, the lower rack or slot takes control.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

Use **ipv4 conflict-policy** command to set an IPARM policy that resolves a conflict in the configured addresses. The policy tells IPARM what address to select from the addresses in conflict. The policy then forces the address in conflict to become inactive.

Task ID

Task ID	Operations
ipv4	read, write
ip-services	read, write

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

```
RP/0/0/CPU0:router(config)# ipv6 conflict-policy static
```

Related Commands

Command	Description
show arm conflicts, on page 61	Displays the IPv4 or IPv6 address conflict information.

ipv4 directed-broadcast

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

ipv4 directed-broadcast

no ipv4 directed-broadcast

Syntax Description

This command has no keywords or arguments.

Command Default

By default, directed broadcasts are dropped.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to enable the forwarding of IPv4 directed broadcasts on interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface gigabitethernet  0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv4 directed-broadcast
```

Related Commands

Command	Description
ipv4 unnumbered (point-to-point), on page 20	Enables IP processing on a point-to-point interface without assigning an explicit IP address to the interface.
show ipv4 interface , on page 72	Lists a summary of IPv4 information and status for the interface.

ipv4 helper-address

To configure the address to which the software forwards User Datagram Protocol (UDP) broadcasts, received on an interface, use the **ipv4 helper-address** command in interface configuration mode. To remove an IPv4 helper address, use the **no** form of this command.

{**ipv4 helper-address** [**vrf** *vrf-name*]| [*destination-address*]}

{**no ipv4 helper-address** [**vrf** *vrf-name*]| [*destination-address*]}

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
destination-address	Destination broadcast or host address to be used when UDP broadcasts are forwarded. There can be more than one helper address per interface.

Command Default

IPv4 helper addresses are disabled. Default VRF is assumed if the VRF is not specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

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.

A DHCP relay profile must be configured to perform DHCP Relay. The **ip helper-address** command is used to forward broadcast UDP (non-DHCP) packets.

Note To configure the address to which the software forwards BOOTP broadcasts, use the **helper-address** command in the DHCP IPv4 profile relay configuration submode. For more information, see the **helper-address** command in the DHCP Commands chapter.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to specify that all UDP broadcast packets received on POSinterface 0/1/1/0 are forwarded to 192.168.1.0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/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 softwareto respond to IPv4 Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ipv4 mask-reply** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipv4 mask-reply

no ipv4 mask-reply

Syntax Description This command has no keywords or arguments.

Command Default IPv4 mask replies are not sent.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example enables the sending of ICMP mask reply messages on POSinterface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/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 an appropriate configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv4 mtu *bytes*

no ipv4 mtu

Syntax Description

bytes	MTU in bytes. Range is 68 to 65535 bytes for IPv4 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

Command Default

If no MTU size is configured for IPv4 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, if the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IPv4 MTU value. If the current IPv4 MTU value is the same as the MTU value, and you change the MTU value, the IPv4 MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IPv4 MTU value has no effect on the value for the **mtu** command.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

This example shows how to set the maximum IPv4 packet size for POS interface 0/1/1/0 to 300 bytes:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv4 mtu 300
```

Related Commands

Command	Description
show ipv4 interface , on page 72	Displays the MTU status of interfaces configured for IPv4.

ipv4 redirects

To enable the sending of IPv4 Internet Control Message Protocol (ICMP) redirect messages if the software is forced to resend a packet through the same interface on which it was received, use the **ipv4 redirects** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipv4 redirects

no ipv4 redirects

Syntax Description This command has no keywords or arguments.

Command Default 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 3.2	This command was introduced.

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

ICMP redirect messages are disabled by default on the interface unless the Hot Standby Router Protocol (HSRP) is configured.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to disable the sending of ICMP IPv4 redirect messages on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv4 redirects
```

ipv4 source-route

To allow the processing of any IPv4 datagrams containing a source-route header option, use the **ipv4 source-route** command in global configuration mode. To have the software discard any IP datagram that contains a source-route option, use the **no** form of this command.

ipv4 source-route

no ipv4 source-route

Syntax Description This command has no keywords or arguments.

Command Default The software discards any IPv4 datagrams containing a source-route header option.

Command Modes Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	The following sections were modified: • Command description • Defaults • Usage Guidelines

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

By default, any IPv4 datagram which contains a source-route header option is discarded.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to allow the processing of any IPv4 datagrams containing a source-route header option:

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

ipv4 unnumbered (point-to-point)

To enable IPv4 processing on a point-to-point interface without assigning an explicit IPv4 address to that interface, use the **ipv4 unnumbered** command in an appropriate configuration mode. To disable this feature, use the **no** form of this command.

ipv4 unnumbered *interface-type interface-instance*

no ipv4 unnumbered *interface-type interface-instance*

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-instance	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

IPv4 processing on a point-to-point interface is disabled unless an IPv4 address is assigned explicitly to that interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IPv4 packet. It also uses the IPv4 address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- Packet-over-SONET (POS) interfaces using High-Level Data Link Control (HDLC), PPP, and tunnel interfaces can be unnumbered.

- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.

The interface you specify by the *interface-type* and *interface-number* arguments must be enabled (listed as "up" in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a POS interface, you should configure the POS interface as unnumbered. This strategy allows you to conform to RFC 1195, which states that IP addresses are not required on each interface.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

In this example the GigabitEthernet interface 0/1/1/0 is assigned the loopback interface address 5:

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

ipv4 unreachables disable

To disable the generation of IPv4 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv4 unreachables disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv4 unreachables disable

no ipv4 unreachables disable

Syntax Description This command has no keywords or arguments.

Command Default IPv4 ICMP unreachables messages are generated.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

If the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP protocol unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects a number of ICMP unreachable messages.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write
config-services	read, write

This example shows how to disable the generation of ICMP unreachable messages on POSinterface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv4 unreachables disable
```

ipv4 virtual address

To define an IPv4 virtual address for a network of management Ethernet interfaces, use the **ipv4 virtual interface** command in global configuration mode. To remove an IPv4 virtual address from the configuration, use the **no** form of this command.

ipv4 virtual address {[**vrf** *vrf-name*] *ipv4-address*/*mask*| **use-as-src-addr**}

no ipv4 virtual address {[**vrf** *vrf-name*] *ipv4-address*/*mask*| **use-as-src-addr**}

Syntax Description

vrf *vrf-name*	(Optional) Configures the virtual address on a per VPN routing and forwarding (VRF) basis for the management interfaces The *vrf-name* argument specifies the name of the VRF.
ipv4 address	Virtual IPv4 address and the mask that is to be unconfigured.

mask	Mask for the associated IP subnet. The network mask can be specified in either of two ways: • The network mask can be a four-part dotted-decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address. A slash between numbers is required as part of the notation.
use-as-src-addr	Enables the virtual address to be used as the default SRC address on sourced packets.

Command Default

No IPv4 virtual address is defined for the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	The **use-as-src-addr** keyword was added.

Usage Guidelines

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

Configuring an IPv4 virtual address enables you to access the router from a single virtual address with a management network. An IPv4 virtual address persists across route processor (RP) failover situations.

Configuring an IPv4 virtual address enables you to access a dual RP router from a single address without prior knowledge of which RP is active. An IPv4 virtual address persists across RP failovers. For this to happen, the virtual IPv4 address must share a common IPv4 subnet with a Management Ethernet interface on both RPs. On a Cisco XR 12000 router, in which each RP has multiple Management Ethernet interfaces (two on PRP-1 or three on PRP-2), the virtual IPv4 address maps to whichever Management Ethernet interface on the active RP with which it shares a common IP subnet.

If you disable the **ipv4 virtual address** command with the **vrf** keyword, the virtual IP address is unconfigured for the corresponding VRF or for the default if no VRF is specified. This results in the removal of the entry for the virtual IP address in the VRF table and in the ARP cache.

The default VRF is chosen when no VRF is specified. The virtual IP address is activated on a management interface that is attached to a default VRF.

The **use-as-src-addr** keyword eliminates the need for configuring a loopback interface as the source interface (that is, update source) for management applications. When an update source is not configured, management

applications allow the transport processes (TCP, UDP, raw_ip) to pick a suitable source address. The transport processes, in turn, consult the FIB to do so. If a Management Ethernet's IP address is picked as the source address and if the **use-as-src-addr keyword** is configured, then the transport processes replace the Management Ethernet's IP address with a relevant virtual IP address. This functionality works across RP switchovers.

Task ID

Task ID	Operations
ipv4	read, write
network	read, write

The following example shows how to define an IPv4 virtual address:

```
RP/0/0/CPU0:router(config)# ipv4 virtual address 10.3.32.154/8
```

The following example show how to configure the virtual IP addresses for management interfaces on a per VRF basis:

```
RP/0/0/CPU0:router(config)# ipv4 virtual address vrf ppp 12.26.3.4/16
```

ipv6 address

To configure an IPv6 address for an interface and enable IPv6 processing on the interface using an EUI-64 interface ID in the low-order 64 bits of the address, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix*/*prefix-length* **[eui-64]** [**route-tag** *route-tag value*]

no ipv6 address *ipv6-prefix*/*prefix-length* **[eui-64]** [**route-tag** *route-tag value*]

Syntax Description

ipv6-prefix	The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
eui-64	(Optional) Specifies an interface ID in the low-order 64 bits of the IPv6 address.
route-tag	(Optional) Specifies that the configured address has a route tag to be associated with it.
route-tag value	(Optional) Value of the route tag. Range is 1 to 4294967295.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.
Release 3.8.0	The **route-tag** keyword was added.

Usage Guidelines

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

If the value specified for the / *prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS XR software detects another host using one of its IPv6 addresses, it displays an error message on the console.

The route-tag feature attaches a tag to all IPv6 addresses. The tag is propagated from the Management Agents (MA) to the Address Repository Managers (RPM) to routing protocols, thus enabling the user to control the redistribution of connected routes by looking at the route tags via RPL scripts.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

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/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Related Commands

Command	Description
ipv6 address link-local, on page 27	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.

Command	Description
show ipv6 interface , on page 79	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** [**route-tag** *route-tag value*]

no ipv6 address *ipv6-address* **link-local** [**route-tag** *route-tag value*]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-local	Specifies a link-local address. The *ipv6-address* value specified with this command overrides the link-local address that is automatically generated for the interface.
route-tag	(Optional) Specifies that the configured address has a route-tag to be associated with it.
route-tag value	(Optional) Displays the route-tag value. Range is 1 to 4294967295.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	The **route-tag** keyword was added.

Usage Guidelines

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

If the Cisco IOS XR software detects another host using one of its IPv6 addresses, the software displays an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 address link-local** command.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

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/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

Related Commands

Command	Description
ipv6 address, on page 25	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 , on page 79	Displays the usability status of interfaces configured for IPv6.

ipv6 assembler

To configure the maximum number of packets that are allowed in assembly queues or to configure the number of seconds an assembly queue will hold before timeout , use the **ipv6 assembler** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

ipv6 assembler {**max-packets** *value* | **timeout** *seconds*}

no ipv6 assembler {**max-packets** *value* | **timeout** *seconds*}

Syntax Description

max-packets	Maximum packets allowed in assembly queues.
timeout	Number of seconds an assembly queue will hold before timeout.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.
	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ipv6	read, write

Example

The following example shows how to configure the maximum number of packets that are allowed in assembly queues:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# ipv6 assembler max-packets 100
```

Related Commands

Command	Description
ipv4 assembler max-packets, on page 10	Configures the maximum number of packets that are allowed in assembly queues
ipv4 assembler max-packets, on page 10	Configures the maximum number of packets that are allowed in assembly queues

ipv6 conflict-policy

To enable IP Address Repository Manager (IPARM) conflict resolution, use the **ipv6 conflict-policy** command in global configuration mode. To disable the IPARM conflict resolution, use the **no** form of the command.

ipv6 conflict-policy {**highest-ip**| **longest-prefix**| **static**}

no ipv6 conflict-policy {**highest-ip**| **longest-prefix**| **static**}

Syntax Description

highest-ip	Keeps the highest IP address in the conflict set.
longest-prefix	Keeps the longest prefix match in the conflict set.
static	Keeps the existing interface running across new address configurations.

Command Default

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.

Usage Guidelines

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

Task ID

Task ID	Operations
ipv6	read, write
ip-services	read, write

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

```
RP/0/0/CPU0:router(config)# ipv6 conflict-policy longest-prefix
```

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in an appropriate configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example shows how to enable IPv6 processing on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 enable
```

Related Commands

Command	Description
show ipv6 interface , on page 79	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.

Command Default

hops : 64 hops

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

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/0/0/CPU0:router(config)# ipv6 hop-limit 15
```

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages on all nodes, use the **ipv6 icmp error-interval** command in global configuration mode. To return the interval to its default setting, use the **no** form of this command.

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

Syntax Description

milliseconds	Time interval (in milliseconds) between tokens being placed in the bucket. Range is 0 to 2147483647.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is 1 to 200 with a default of 10 tokens.

Command Default

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero.

milliseconds : 100 milliseconds

bucketsize : 10 tokens

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

Use the **ipv6 icmp error-interval** command in global configuration mode to limit the rate at which IPv6 ICMP error messages are sent for each node. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens being placed in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens stored in the bucket. Tokens are removed

from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* argument is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Use the **show ipv6 traffic** EXEC command to display IPv6 ICMP rate-limited counters.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
RP/0/0/CPU0:router(config)# ipv6 icmp error-interval 50 20
```

Related Commands

Command	Description
show ipv6 neighbors , on page 88	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 an appropriate configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*

no ipv6 mtu

Syntax Description

bytes	MTU in bytes. Range is 1280 to 65535 for IPv6 packets. The maximum MTU size that can be set on an interface depends on the interface medium.

Command Default

If no MTU size is configured for IPv6 packets sent on an interface, the interface derives the MTU from the Layer 2 MTU.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

If an IPv6 packet exceeds the MTU set for the interface, only the source router of the packet can fragment it.

The maximum MTU size that can be set on an interface depends on the interface medium. If the Layer 2 MTU is smaller than the Layer 3 MTU, the Cisco IOS XR software uses the Layer 2 MTU value for the Layer 3 MTU. Conversely, If the Layer 3 MTU is smaller than the Layer 2 MTU, the software uses Layer 3 MTU value. In other words the Cisco IOS XR software uses the lower of the two values for the MTU.

All devices on a physical medium must have the same protocol MTU to operate.

Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IPv6 MTU value. If the current IPv6 MTU value is the same as the MTU value, and you change the MTU value, the IPv6 MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IPv6 MTU value has no effect on the value for the **mtu** command.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example shows how to set the maximum IPv6 packet size for POS interface 0/1/1/0 to 1350 bytes:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 mtu 1350
```

Related Commands

Command	Description
show ipv6 interface , on page 79	Displays the usability status of interfaces configured for IPv6.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface, use the **ipv6 nd dad attempts** command in an appropriate configuration mode. To return the number of messages to the default value, use the **no** form of this command.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts *value*

Syntax Description

value	Number of neighbor solicitation messages. Range is 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Command Default

Duplicate address detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled. The default is one message.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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 POS
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to duplicate.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Duplicate address detection is performed on all multicast-enabled IPv6 interfaces, including the following interface types:

- Cisco High-Level Data Link Control (HDLC)
- Ethernet, FastEthernet, and GigabitEthernet
- PPP

Task ID

Task ID	Operations
ipv6	read, write
config-services	read, write

This example shows how to set the number of consecutive neighbor solicitation messages for interface 0/2/0/1 to 1 and then display the state (tentative or duplicate) of the unicast IPv6 address configured for an interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface POS 0/2/0/1
```

```
RP/0/0/CPU0:router(config-if)# ipv6 nd dad attempts 1
RP/0/0/CPU0:router(config-if)# Uncommitted changes found, commit them before
exiting(yes/no/cancel)? [cancel]:y

RP/0/0/CPU0:router# show ipv6 interface
POS2/2/0/0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
POS2/2/0/1 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.
POS2/2/0/2 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 , on page 39	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface , on page 79	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 an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Syntax Description This command has no keywords or arguments.

Command Default The managed address configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

Setting the managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example shows how to configure the managed address configuration flag in IPv6 router advertisements on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 interface , on page 79	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 an appropriate configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Syntax Description

milliseconds	Interval (in milliseconds) between IPv6 neighbor solicit transmissions. Range is 1000 to 3600000.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements, and the value 1000 is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

This value is included in all IPv6 router advertisements sent out from this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface , on page 79	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 an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note If the managed address configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the other stateful configuration flag.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example configures the "other stateful configuration" flag in IPv6 router advertisements on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag , on page 38	Sets the managed address configuration flag in IPv6 router advertisements.
show ipv6 interface , on page 79	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-adv	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.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

To control how prefixes are advertised, use the **ipv6 nd prefix** command. By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised with default values. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, only the specified prefixes are advertised with the configured values, all other prefixes are advertised with default values.

The default keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix is no longer advertised.

When onlink is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

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/0/0/CPU0:router(config)# interface POS 0/1/0/0
RP/0/0/CPU0:router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

Related Commands

Command	Description
ipv6 address, on page 25	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, on page 27	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 nd managed-config-flag , on page 38	Sets the managed address configuration flag in IPv6 router advertisements.
show ipv6 interface , on page 79	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in an appropriate configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval *seconds*

no ipv6 nd ra-interval *seconds*

Syntax Description

seconds	The interval (in seconds) between IPv6 router advertisement transmissions.

Command Default

seconds : 200 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the router is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example configures an IPv6 router advertisement interval of 201 seconds on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime , on page 46	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface , on page 79	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 an appropriate configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Syntax Description

seconds	The validity (in seconds) of this router as a default router on this interface.

Command Default

seconds : 1800 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

The router lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The router lifetime value can be set to a nonzero value to indicate that it should be considered a default router on this interface. The nonzero value for the router lifetime value should not be less than the router advertisement interval.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example configures an IPv6 router advertisement lifetime of 1801 seconds on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
```

```
RP/0/0/CPU0:router(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval , on page 44	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface , on page 79	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in an appropriate configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Syntax Description

milliseconds	The amount of time (in milliseconds) that a remote IPv6 node is considered reachable. The range is from 0 to 3600000.

Command Default

0 milliseconds (unspecified) is advertised in router advertisements and 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was supported .
Release 3.6.0	The range value was added for the *milliseconds* argument.

Usage Guidelines

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

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 indicates that the configured time is unspecified by this router.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example shows how to configure an IPv6 reachable time of 1,700,000 milliseconds for POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface , on page 79	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 keywords or arguments.

Command Default The default value is disabled.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

The following example shows how to redirect IPv6 nd-directed broadcasts on POS interface 0/2/0/2:

```
RP/0/0/CPU0:router(config)# interface POS 0/0/0/0
0/2/0/2
RP/0/0/CPU0:router(config-if)# ipv6 nd redirects
```

Related Commands

Command	Description
show ipv6 interface , on page 79	Displays the usability status of interfaces configured for IPv6.

ipv6 nd scavenge-timeout

To set the lifetime for neighbor entries in the stale state, use the **ipv6 nd scavenge-timeout** command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd scavenge-timeout *seconds*

no ipv6 nd scavenge-timeout *seconds*

Syntax Description

seconds	RA lifetime in seconds. The range is from 0 to 43200.

Command Default

No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

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

When the scavenge-timer for a neighbor entry expires, the entry is cleared.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

The following example shows how to set the lifetime for the neighbor entry:

```
RP/0/0/CPU0:router(config)# ipv6 nd scavenge-timeout 3000
```

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in an appropriate configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description This command has no keywords or arguments.

Command Default IPv6 router advertisements are automatically sent on other types of interlaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example shows how to suppress IPv6 router advertisements on POS interface 0/1/1/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/1/1/0
RP/0/0/CPU0:router(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface , on page 79	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static IPv6 entry from the IPv6 neighbors discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*

Syntax Description

ipv6-address	The IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-instance	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
hardware-address	The local data-link address (a 48-bit address).

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

The **ipv6 neighbor** command is similar to the **arp** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

Use the **show ipv6 neighbors** command to display static entries in the IPv6 neighbors discovery cache. A static entry in the IPv6 neighbor discovery cache has one state: reach (reachable)—The interface for this entry is up. If the interface for the entry is down, the **show ipv6 neighbors** command does not show the entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the reach (reachable) state are different for dynamic and static cache entries. See the **show ipv6 neighbors** command for a description of the reach (reachable) state for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbors discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to reach [reachable]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Note Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write

The following example shows how to configure a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on ethernet interface 0/ 0/CPU0/0:

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

Related Commands

Command	Description
clear ipv6 neighbors , on page 4	Deletes all entries in the IPv6 neighbors discovery cache, except static entries.
ipv6 enable , on page 31	Disables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
show ipv6 neighbors , on page 88	Displays IPv6 neighbors discovery cache information.

ipv6 source-route

To enable processing of the IPv6 type source (type 0) routing header, use the **ipv6 source-route** command in global configuration mode. To disable the processing of this IPv6 extension header, use the **no** form of this command.

ipv6 source-route

no ipv6 source-route

Syntax Description

This command has no keywords or arguments.

Command Default

The **no** version of the **ipv6 source-route** command is the default.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

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

The **no ipv6 source-route** command (which is the default) prevents hosts from performing source routing using your routers. When the **no ipv6 source-route** command is configured and the router receives a packet with a type 0 source routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.

Task ID

Task ID	Operation
network	read, write
ipv6	read, write

Example

The following example shows how to allow the processing of any IPv6 datagrams containing a source-route header option:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# ipv6 source-route
RP/0/0/CPU0:router(config)#
```

Related Commands

Command	Description
ipv4 source-route, on page 19	Allow the processing of any IPv4 datagrams containing a source-route header option.

ipv6 unreachables disable

To disable the generation of IPv6 Internet Control Message Protocol (ICMP) unreachable messages, use the **ipv6 unreachables disable** command in an appropriate configuration mode. To re-enable the generation of ICMP unreachable messages, use the **no** form of this command.

ipv6 unreachables disable

no ipv6 unreachables disable

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 ICMP unreachables messages are generated.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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

If the software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP protocol unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects a number of ICMP unreachable messages.

Task ID

Task ID	Operations
ipv6	read, write
network	read, write
config-services	read, write

This example shows how to disable the generation of ICMP unreachable messages on POS interface 0/6/0/0:

```
RP/0/0/CPU0:router(config)# interface POS 0/6/0/0
RP/0/0/CPU0:router(config-if)# ipv6 unreachables disable
```

local pool

To create one or more local address pools from which IP addresses are assigned when a peer connects, use the **local pool** command in global configuration mode. To restore the default behavior, use the **no** form of this command.

local pool [ipv4] [**vrf** *vrf_name*] {*poolname*| **default**} *first-ip-address* [*last-ip-address*]

no local pool [**ipv4**] [**vrf** *vrf_name*] {*poolname*| **default**} *first-ip-address* [*last-ip-address*]

Syntax Description

vrf	Specifies that a VRF name will be given. If is parameter is missing, the default VRF is assumed.
vrf_name	Specifies the name of the VRF to which the addresses of the pool belongs. If no name is given, the default VRF is assumed.
default	Creates a default local IPv4 address pool that is used if no other pool is named.
poolname	Specifies the name of the local IPv4 address pool.
first-ip-address	Specifies the first address in an IPv4 address range. If high-IP-address is not specified, the address range is considered to have only one address.
last-ip-address	(Optional) Specifies the last address in an IPv4 address range. If high-IP-address is not specified, the address range is considered to have only one address.

Command Default

Special default pool if VRF is not specified. By default, this functionality is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

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

Use this command to create local address pools to use in assigning IP addresses when a peer connects. You can also add range of IP addresses to an existing pool. If no pool name is specified, the pool with the name "default" is used.

The optional **vrf** keyword and associated *vrf name* allows the association of an IPv4 address pool with a named VRF. Any IPv4 address pool created without the **vrf** keyword automatically becomes a member of a default VRF. An IPv4 address pool name can be associated with only one VRF. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IPv4 address pool name with a different VRF is rejected. Therefore, each use of a pool name is an implicit selection of the associated VRF.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the default pool only in the default VRF.

All IPv4 address pools within a VRF are checked to prevent overlapping addresses; however, addresses may overlap across different VRFs.

Task ID

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

The following example creates a local IPv4 address pool named “pool2,” which contains all IPv4 addresses in the range 172.16.23.0 to 172.16.23.255:

```
RP/0/0/CPU0:router(config)# local pool ipv4 pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
RP/0/0/CPU0:router(config)#no local pool ipv4 default
RP/0/0/CPU0:router(config)#local pool ipv4 default 10.1.1.0 10.1.4.255
```

Note It is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IPv4 addresses. To extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IPv4 addresses into one pool:

```
RP/0/0/CPU0:router(config)#local pool ipv4 default 10.1.1.0 10.1.9.255
RP/0/0/CPU0:router(config)#local pool ipv4 default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IPv4 address pools in the base system group:

```
RP/0/0/CPU0:router(config)#local pool vrf grp1 ipv4 p1_g1 10.1.1.1 10.1.1.50
RP/0/0/CPU0:router(config)#local pool vrf grp1 ipv4 p2_g1 10.1.1.100 10.1.1.110
RP/0/0/CPU0:router(config)#local pool vrf grp2 ipv4 p1_g2 10.1.1.1 10.1.1.40
RP/0/0/CPU0:router(config)#local pool ipv4 lp1 10.1.1.1 10.1.1.10
RP/0/0/CPU0:router(config)#local pool vrf grp1 ipv4 p3_g1 10.1.2.1 10.1.2.30
RP/0/0/CPU0:router(config)#local pool vrf grp2 ipv4 p2_g2 10.1.1.50 10.1.1.70
RP/0/0/CPU0:router(config)#local pool ipv4 lp2 10.1.2.1 10.1.2.10
```

In this example:

- VRF grp1 consists of pools p1_g1, p2_g1, and p3_g1.
- VRF grp2 consists of pools p1_g2 and p2_g2.
- Pools lp1 and lp2 are not explicitly associated with a vrf and are therefore members of the default vrf.

Note IPv4 address 10.1.1.1 overlaps in vrfs grp1, grp2 and the default vrf . There is no overlap within any vrf that includes the default vrf.

The VPN requires a configuration that selects the proper vrf by selecting the proper pool based on remote user data. Each user in a given VPN can select an address space using the pool and associated vrf appropriate for that VPN. Duplicate addresses in other VPNs (other vrfs) are not a concern, because the address space of a VPN is specific to that VPN. In the example, a user in VRF vpn1 is associated with a combination of the pools p1_vpn1, p2_vpn1, and p3_vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

remote-route-filtering

To disable remote route filtering on a vrf for SVD core-facing cards, use the **remote-route-filtering** command in the VRF configuration mode. To enable remote route filtering, use the **no** form of this command.

remote-route-filtering disable

no remote-route-filtering disable

Syntax Description

disable	Disables remote route filtering per VRF.

Command Default By default, remote route filtering on a vrf is enabled.

Command Modes VRF configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

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

Task ID

Task ID	Operation
ip-services	read, write

Example

This example shows how to disable remote route filtering on a vrf for SVD core-facing cards, using the **remote-route-filtering** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vrf vrf-1
RP/0/0/CPU0:router(config-vrf)# remote-route-filtering disable
RP/0/0/CPU0:router(config-vrf)#
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

selective-vrf-download

To download locally significant tables on a customer-facing card, or to disable selective VRF download, use the **selective-vrf-download** command in global configuration mode. To disable this feature, use the **no** form of this command.

selective-vrf-download [**location** *location* **vrf-group** *group-name*] | [**disable**]

no selective-vrf-download [**location** *location* **vrf-group** *group-name*] | [**disable**]

Syntax Description

location *location*	Configures selective vrf-download on specified location.
vrf-group *group-name*	Downloads tables corresponding to the vrfs of the specified vrf-group.
disable	Disables selective VRF download.

Command Default

If selective VRF download is supported by the router, then, by default, **selective-vrf-download** is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

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

For a location, only one vrf group is supported.

Task ID

Task ID	Operation
ip-services	read, write

Example

This example shows how to download locally-significant routes on a customer facing router, using the **selective-vrf-download** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# selective-vrf-download location 0/2/CPU0 vrf-group group1
RP/0/0/CPU0:router(config-svd)#
```

This example shows how to disable selective VRF download, using the **selective-vrf-download** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# selective-vrf-download disable
RP/0/0/CPU0:router(config-svd)#
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

show arm conflicts

To display IPv4 or IPv6 address conflict information identified by the Address Repository Manager (ARM), use the **show arm conflicts** command in EXEC mode.

show arm {**ipv4**| **ipv6**} [**vrf** *vrf-name*] **conflicts** [**address**| **override**| **unnumbered**]

Syntax Description

ipv4	Displays IPv4 address conflicts.
ipv6	Displays IPv6 address conflicts.
vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information. Available for IPv4 only.
vrf-name	(Optional) Name of a VRF.
address	(Optional) Displays address conflict information.
override	(Optional) Displays address conflict override information.
unnumbered	(Optional) Displays unnumbered interface conflict information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Use the **show arm conflicts** command to display information about IPv4 or IPv6 address conflicts. You can use address conflict information to identify misconfigured IPv4 or IPv6 addresses.

Conflict information is displayed for interfaces that are forced down and for interfaces that are up.

Issuing the **show arm conflicts** command without specifying any optional keywords displays the output generated from both the **address** and **unnumbered** keywords.

Task ID

Task ID	Operations
network	read

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

```
RP/0/0/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/0/0/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/0/0/CPU0:router# show arm ipv4 conflicts unnumbered

Forced down interface          Up interface                   VRF
tu2->tu1                       tu1->Lo1
```

This table describes the significant fields shown in the display.

Table 1: show arm conflicts Command Field Descriptions

Field	Description
Forced down	Legend defining a symbol that may appear in the output for this command.
Down interface & addr	Forced down interface name, type, and address.

Field	Description
Up interface & addr	List of interfaces that are up.
Forced down interface	Unnumbered interfaces that are in conflict and forced down.
Up interface	Unnumbered interfaces that are in conflict and are up.

show arm database

To display IPv4 or IPv6 address information stored in the Address Repository Manager (ARM) database, use the **show arm database** command in EXEC mode.

show arm {**ipv4**| **ipv6**} [**vrf** *{vrf-name}*] **database** [**interface** *type interface-path-id*| **network** *prefix*/*length*]

Syntax Description

ipv4	Displays IPv4 address information.
ipv6	Displays IPv6 address information.
vrf	Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
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.
interface-path-id	Physical interface or virtual interface. **Note** Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
network	Displays addresses that match a prefix.
prefix / *length*	Network prefix and mask. A slash (/) must precede the specified mask. The range is from 0 to 128.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was supported.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

The **show arm database** command should be used to display information in the IP ARM database. Database information is displayed with the IPv4 or IPv6 address, interface type and name, and producer information.

Task ID

Task ID	Operations
network	read

The following is sample output from the **show arm database** command:

```
RP/0/0/CPU0:router# show arm
 database
Fri Jul 25 10:54:52.304 PST DST

P = Primary, S = Secondary address
|U = Unnumbered
|| Address            Interface
Producer         Route-tag
VRF: default
P  172.29.52.75/24    MgmtEth0/RP0/CPU0/0           ipv4_ma 0/RP0/CPU0         100
P  10.2.2.2/32        Loopback0                     ipv4_ma 0/RP1/CPU0
P  10.12.24.2/24      Bundle-POS24                  ipv4_ma 0/RP1/CPU0
P  10.12.28.2/24      Bundle-Ether28                ipv4_ma 0/RP1/CPU0
P  10.12.29.2/24      Bundle-Ether28.1              ipv4_ma 0/RP1/CPU0
P  10.12.30.2/24      Bundle-Ether28.2              ipv4_ma 0/RP1/CPU0
P  10.12.31.2/24      Bundle-Ether28.3              ipv4_ma 0/RP1/CPU0
P
172.
29.
52.
76/24    MgmtEth0/RP1/CPU0/0  ipv4_ma 0/RP1/CPU0P  10.
112.
12.
2/24     TenGigE0/1/1/0 ipv4_ma 0/1/CPU0

| Address            Interface  Producer
P  10.12.16.2/24      GigabitEthernet0/1/5/0        ipv4_ma 0/1/CPU0           1001
P  10.23.4.2/24       GigabitEthernet0/1/5/1        ipv4_ma 0/1/CPU0           1002
P  10.27.4.2/24       GigabitEthernet0/1/5/2        ipv4_ma 0/1/CPU0
P  10.12.8.2/24       POS0/1/0/1                    ipv4_ma 0/1/CPU0
P  10.112.4.2/24      POS0/1/0/2                    ipv4_ma 0/1/CPU0
P  10.112.8.2/24      POS0/1/0/3                    ipv4_ma 0/1/CPU0
P  10.12.32.2/24      POS0/1/4/2                    ipv4_ma 0/1/CPU0
```

```
P  10.12.32.2/24      POS0/1/4/3                    ipv4_ma 0/1/CPU0
P  172.29.52.28/24    MgmtEth0/4/CPU1/0             ipv4_ma 0/4/CPU1
P  172.29.52.27/24    MgmtEth0/4/CPU0/0             ipv4_ma 0/4/CPU0
P  10.12.20.2/24      GigabitEthernet0/6/5/1        ipv4_ma 0/6/CPU0
P  10.
12.
40.
2/24 GigabitEthernet0/6/5/7 ipv4_ma 0/6/CPU0
S 10.4.2.4/24         gigabitethernet 10/0  ipv4_io 1 10
S 10.4.3.4/24         gigabitethernet 10/1  ipv4_io 1 10

P = Primary, S = Secondary address

|U = Unnumbered

|| Address            Interface                     Producer
VRF: default
P  10.12.12.2/24      POS0/6/0/1                    ipv4_ma 0/6/CPU0
P  10.23.8.2/24       POS0/6/4/4                    ipv4_ma 0/6/CPU0
P  10.12.4.2/24       POS0/6/4/5                    ipv4_ma 0/6/CPU0
P  10.24.4.2/24       POS0/6/4/6                    ipv4_ma 0/6/CPU0
P
10.27.
8.2/24POS0/6/4/7 ipv4_ma 0/6/CPU0
```

This table describes the significant fields shown in the display.

Table 2: show arm database Command Field Descriptions

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

show arm router-ids

To display the router identification information with virtual routing and forwarding table information for the Address Repository Manager (ARM), use the **show arm router-ids** command in EXEC mode.

show arm [ipv4] router-ids

Syntax Description

ipv4	(Optional) Displays IPv4 router information.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.5.0	The **ipv6** and **vrf** keywords were removed.

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

Use the **show arm router-ids** command with the **ipv4** keyword to display the selected router ID information for the router.

Task ID

Task ID	Operations
network	read

The following is sample output from the **show arm router-ids** command:

```
RP/0/0/CPU0:router# show arm router-ids

Router-ID         Interface

10.10.10.10       Loopback0
```

This table describes the significant fields shown in the display.

Table 3: show arm router-ids Command Field Descriptions

Field	Description
Router-ID	Router identification.
Interface	Interface identification.

show arm registrations producers

To display producer registration information for the Address Repository Manager (ARM), use the **show arm registrations producers** command in EXEC mode.

show arm {**ipv4**| **ipv6**} **registrations producers**

Syntax Description

ipv4	Displays IPv4 producer registration information.
ipv6	Displays IPv6 producer registration information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
network	read

The following is sample output from the **show arm registrations producers** command:

```
RP/0/0/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
```

This table describes the significant fields shown in the display.

Table 4: show arm registrations producers Command Field Descriptions

Field	Description
Id	An identifier used by the IP Address ARM (IP ARM) to keep track of the producer of the IP address.
Node	The physical node (RP/LC CPU) where the producer is running.
Producer Id	The string used by the producer when registering with IP ARM.
IPC Version	Version of the apis used by the producer to communicate with IP ARM.
Connected?	Status of whether the producer is connected or not.

show arm summary

To display summary 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 summary information.
ipv6	Displays IPv6 summary information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
network	read

The following is sample output from the **show arm summary** command:

```
RP/0/0/CPU0:router# show arm ipv4 summary

IPv4 Producers                          :    5
IPv4 Router id consumers                :    7
IPv4 address conflicts                  :    2
IPv4 unnumbered interface conflicts     :    1
```

This table describes the significant fields shown in the display.

Table 5: show arm summary Command Field Descriptions

Field	Description
IPv4 Producers	Number of IPv4 producers on the router.
IPv4 address conflicts	Number of IPv4 address conflicts on the router.
IPv4 unnumbered interface conflicts	Number of IPv4 conflicts on unnumbered interfaces.
IPv4 DB Master version	IPv4 DB Master version

show arm vrf-summary

To display a summary of VPN routing and forwarding (VRF) instance information identified by the Address Repository Manager (ARM), use the **show arm vrf-summary** command in EXEC mode.

show arm {**ipv4**| **ipv6**} **vrf-summary**

Syntax Description

ipv4	Displays IPv4 address information.
ipv6	Displays IPv6 address information.

Command Default

None

Command Modes EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.
Release 3.6.0	The **ipv4** and **ipv6** keywords were added.

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

Use the **show arm vrf-summary** command to display information about an IPv4 VPN routing and forwarding instance.

Task ID

Task ID	Operations
network	read

The following example is output from the **show arm vrf-summary** command:

```
RP/0/0/CPU0:router# show arm vrf-summary

VRF IDs:        VRF-Names:
0x60000000      default
0x60000001      vrf1
0x60000002      vrf2
```

This table describes the significant fields shown in the display.

Table 6: show arm vrf-summary Command Field Descriptions

Field	Description
VRF IDs	VPN routing and forwarding (VRF) identification (vrfid) number.
VRF-Names	Name given to the VRF.

show clns statistics

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

show clns statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was supported.

Usage Guidelines

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

Use this command to display CLNS statistics.

Task ID

Task ID	Operations
isis	read

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

```
RP/0/0/CPU0:router# show clns statistics

CLNS Statistics:
Last counter clear:                    2868 seconds ago
Total number of packets sent:          0
Total number of packets received:      0
Send packets dropped, buffer overflow: 0
Send packets dropped, out of memory:   0
Send packets dropped, other:           0
Receive socket max queue size:         0
Class    Overflow/Max   Rate Limit/Max
IIH             0/0             0/0
LSP             0/0             0/0
SNP             0/0             0/0
OTHER           0/0             0/0
Total          0               0
```

This table describes the significant fields shown in the display.

Table 7: show clns traffic Command Field Descriptions

Field	Description
Class	Indicates the packet type. Packets types are as follows: • IIH—Intermediate System-to-Intermediate-System hello packets • lsp—Link state packets • snp—Sequence number packets • other
Overflow/Max	Indicates the number of packet drops due to the socket queue being overflown. The count displays in an *x/y* format where *x* indicates the total number of packet drops and *y* indicates the maximum number of drops in a row.
Rate Limit/Max	Indicates the number of packet drops due to rate limitation. The count displays in an *x/y* format where *x* indicates the total number of packet drops and *y* indicates the maximum number of drops in a row.

show ipv4 interface

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

show ipv4 [**vrf** *vrf-name*] **interface** [*type interface-path-id*| **brief**| **summary**]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	Interface type. For more information, use the question mark (?) online help function.

interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ 0/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays the primary IPv4 addresses configured on the router's interfaces and their protocol and line states.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

If VRF is not specified, the software displays the default VRF.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

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

The interface name will be displayed only if the name belongs to the VRF instance. If the *vrf-name* is not specified then the interface instance will be displayed only if the interface belongs to the default VRF.

Task ID

Task ID	Operations
ipv4	read
network	read

This is the sample output of the **show ipv4 interface** command:

```
RP/0/0/CPU0:router# show ipv4 interface

Loopback0 is Up, line protocol is Up
  Internet address is
1.0.0.1/
8 with route-tag 110
  Secondary address 10.0.0.1/8
  MTU is 1514 (1514 is available to IP)
  Multicast reserved groups joined: 10.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
POS0/0/0/0 is Up, line protocol is Up
  Internet address is 10.25.58.1/16
  MTU is 1514 (1500 is available to IP)
  Multicast reserved groups joined: 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
POS0/0/0/0 is Shutdown, line protocol is Down
  Vrf is default (vrfid 0x60000000)
  Internet protocol processing disabled
```

This table describes the significant fields shown in the display.

Table 8: show ipv4 interface Command Field Descriptions

Field	Description
Loopback0 is Up	If the interface hardware is usable, the interface is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is Up	If the interface can provide two-way communication, the line protocol is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address	IPv4 Internet address and subnet mask of the interface.
Secondary address	Displays a secondary address, if one has been set.

Field	Description
MTU	Displays the IPv4 MTU[1] value set on the interface.
Multicast reserved groups joined	Indicates the multicast groups this interface belongs to.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled or disabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether proxy ARP[2] is enabled or disabled on an interface.
ICMP redirects	Specifies whether ICMPv4[3] redirects are sent on this interface.
ICMP unreachables	Specifies whether unreachable messages are sent on this interface.
Internet protocol processing disabled	Indicates an IPv4 address has not been configured on the interface.

1 MTU = maximum transmission unit
2 ARP = Address Resolution Protocoladdress resolution protocol
3 ICMPv4 = Internet Control Message Protocol internet control message protocol version 4

show local pool

To display IPv4 local pool details, use the **show local pool** command in EXEC mode.

show {**local**| *other_pool_types*} **pool** [**vrf** *vrf_name*] {**ipv4**| **ipv6**} {**default**| *poolname*}

Syntax Description

local	Specifies that the address pool is local.
vrf	Specifies that a VRF name will be given. If is parameter is missing, the default VRF is assumed.
vrf_name	Specifies the name of the VRF to which the addresses of the pool belongs. If no name is given, the default VRF is assumed.
default	Creates a default local IPv4 address pool that is used if no other pool is named.

poolname	Specifies the name of the local IPv4 address pool.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ipv4	read
network	read

The following is sample output from the **show ipv4 local pool** with a poolname of P1:

```
RP/0/0/CPU0:router# show ipv4 local pool P1

Pool Begin End FreeInUse
P1 172.30.228.11172.30.228.1660
Available addresses:
172.30.228.11
172.30.228.12
172.30.228.13
172.30.228.14
172.30.228.15
172.30.228.16
Inuse addresses:
None
```

This table describes the significant fields shown in the display.

Table 9: show ipv4 local pool Command Descriptions

Field	Description
Pool	Name of the pool.
Begin	First IP address in the defined range of addresses in this pool.

Field	Description
End	Last IP address in the defined range of addresses in this pool.
Free	Number of addresses available.
InUse	Number of addresses in use.

Related Commands

Command	Description
local pool, on page 56	Creates one or more local address pools from which IP addresses are assigned when a peer connects.

show ipv4 traffic

To display the IPv4 traffic statistics, use the **show ipv4 traffic** command in the EXEC mode.

show ipv4 traffic [brief]

Syntax Description

brief	(Optional) Displays only IPv4 and Internet Control Message Protocol version 4 (ICMPv4) traffic.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

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

Task ID

Task ID	Operations
ipv4	read
network	read

This is the sample output of the **show ipv4 traffic** command:

```
RP/0/0/CPU0:router# show ipv4 traffic

IP statistics:
  Rcvd:  16372 total, 16372 local destination
         0 format errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad source, 0 bad header
         0 with options, 0 bad, 0 unknown
  Opts:  0 end, 0 nop, 0 basic security, 0 extended security
         0 strict source rt, 0 loose source rt, 0 record rt
         0 stream ID, 0 timestamp, 0 alert, 0 cipso
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragment count
  Bcast: 0 sent, 0 received
  Mcast: 0 sent, 0 received
   Drop: 0 encapsulation failed, 0 no route, 0 too big, 0 sanity address check
   Sent: 16372 total

ICMP statistics:
  Sent: 0 admin unreachable, 0 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        5 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        5 total
  Rcvd: 0 admin unreachable, 0 network unreachable
        2 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 5 echo reply
        0 mask request, 0 mask reply
        0 redirect, 0 parameter error
        0 source quench, 0 timestamp, 0 timestamp reply
        0 router advertisement, 0 router solicitation
        7 total, 0 checksum errors, 0 unknown

UDP statistics:
        16365 packets input, 16367 packets output
        0 checksum errors, 0 no port
        0 forwarded broadcasts

TCP statistics:
        0 packets input, 0 packets output
        0 checksum errors, 0 no port
```

This table describes the significant fields shown in the display.

Table 10: show ipv4 traffic Command Field Descriptions

Field	Description
bad hop count	Occurs when a packet is discarded because its TTL[4] 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.

4 TTL = time-to-live

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in the EXEC mode.

show ipv6 [**vrf** *vrf-name*] **interface** [**summary** | [*type interface-path-id*][**brief** [**link-local** | **global**]]]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	Interface type. For more information, use the question mark (?) online help function.

interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
link-local	(Optional) Displays the link local IPv6 address.
global	(Optional) Displays the global IPv6 address.
summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	The **summary** keyword was added to the command.
Release 3.5.0	The following modifications are listed for the **show ipv6 interface** command: • The command syntax was modified to be similar to the **show ipv4 interface** command. • The sample output was modified.

Release	Modification
Release 5.1.2	The **link-local** and **global** keywords were added to the command.

Usage Guidelines

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

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

Use the **link-local** or **global** keywords along with the **brief** keyword to view the link local or global IPv6 addresses.

Task ID

Task ID	Operations
ipv6	read

This is the sample output of the **show ipv6 interface** command:

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

GigabitEthernet0/2/0/0 is Up, line protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::212:daff:fe62:c150
  Global unicast address(es):
    202::1, subnet is 202::/64 with route-tag 120
  Joined group address(es): ff02::1:ff00:1 ff02::1:ff62:c150 ff02::2
      ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  access list is not set
```

This table describes the significant fields shown in the display.

Table 11: show ipv6 interface Command Field Descriptions

Field	Description
POS0/3/0/0 is Shutdown, line protocol is Down	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked “Up.” For an interface to be usable, both the interface hardware and line protocol must be up.

Field	Description
line protocol is Up (or down)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful). If the interface can provide two-way communication, the line protocol is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.
TENTATIVE	The state of the address in relation to duplicate address detection. States can be any of the following: • duplicate—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface. • tentative—Duplicate address detection is either pending or under way on this interface. **Note** If an address does not have one of these states (the state for the address is blank), the address is unique and is being used.
Global unicast addresses	Displays the global unicast addresses assigned to the interface.
ICMP redirects	State of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	State of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

Field	Description
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

This is the sample output of the **show ipv6 interface brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 interface brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     fe80::fe:8ff:fecb:26c5        Up         Up
GigabitEthernet0/0/0/1     fe80::4f:88ff:fea0:8c9d       Up         Up
GigabitEthernet0/0/0/3     unassigned                    Shutdown   Down
GigabitEthernet0/0/0/4     unassigned                    Shutdown   Down
```

This is the sample output of the **show ipv6 interface brief global** command:

```
RP/0/0/CPU0:router#show ipv6 interface brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     2001:db8::1                   Up         Up
GigabitEthernet0/0/0/1     2001:db8::2                   Up         Up
GigabitEthernet0/0/0/3     unassigned                    Shutdown   Down
GigabitEthernet0/0/0/4     unassigned                    Shutdown   Down
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 interface gigabitEthernet 0/0/0/0 brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     fe80::fe:8ff:fecb:26c5        Up         Up
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief global** command:

```
RP/0/0/CPU0:router#show ipv6 interface gigabitEthernet 0/0/0/0 brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     2001:db8::1                   Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     fe80::46:c8ff:fe22:daae       Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface brief global** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     2001:db8::2                   Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface** *type interface-path-id* **brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     fe80::46:c8ff:fe22:daae       Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface** *type interface-path-id* **brief global** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     2001:db8::2                  Up         Up
```

Related Commands

Command	Description
show ipv4 interface , on page 72	Displays the usability status of interfaces configured for IPv4.

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in the EXEC mode.

show ipv6 [**vrf** *vrf-name*] **interface** [**summary** | [*type interface-path-id*][**brief** [**link-local** | **global**]]]

Syntax Description

vrf	(Optional) Displays VPN routing and forwarding (VRF) instance information.
vrf-name	(Optional) Name of a VRF.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays the primary IPv6 addresses configured on the router interfaces and their protocol and line states.
link-local	(Optional) Displays the link local IPv6 address.
global	(Optional) Displays the global IPv6 address.

summary	(Optional) Displays the number of interfaces on the router that are assigned, unassigned, or unnumbered.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	The **summary** keyword was added to the command.
Release 3.5.0	The following modifications are listed for the **show ipv6 interface** command: • The command syntax was modified to be similar to the **show ipv4 interface** command. • The sample output was modified.
Release 5.1.2	The **link-local** and **global** keywords were added to the command.

Usage Guidelines

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

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

Use the **link-local** or **global** keywords along with the **brief** keyword to view the link local or global IPv6 addresses.

Task ID

Task ID	Operations
ipv6	read

This is the sample output of the **show ipv6 interface** command:

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

GigabitEthernet0/2/0/0 is Up, line protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::212:daff:fe62:c150
  Global unicast address(es):
    202::1, subnet is 202::/64 with route-tag 120
```

```
Joined group address(es): ff02::1:ff00:1 ff02::1:ff62:c150 ff02::2
    ff02::1
MTU is 1514 (1500 is available to IPv6)
ICMP redirects are disabled
ICMP unreachables are enabled
ND DAD is enabled, number of DAD attempts 1
ND reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
Outgoing access list is not set
Inbound  access list is not set
```

This table describes the significant fields shown in the display.

Table 12: show ipv6 interface Command Field Descriptions

Field	Description
POS0/3/0/0 is Shutdown, line protocol is Down	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is Up (or down)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful). If the interface can provide two-way communication, the line protocol is marked "Up." For an interface to be usable, both the interface hardware and line protocol must be up.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.

Field	Description
TENTATIVE	The state of the address in relation to duplicate address detection. States can be any of the following: • duplicate—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface. • tentative—Duplicate address detection is either pending or under way on this interface. **Note** If an address does not have one of these states (the state for the address is blank), the address is unique and is being used.
Global unicast addresses	Displays the global unicast addresses assigned to the interface.
ICMP redirects	State of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	State of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.

This is the sample output of the **show ipv6 interface brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 interface brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     fe80::fe:8ff:fecb:26c5        Up         Up
GigabitEthernet0/0/0/1     fe80::4f:88ff:fea0:8c9d       Up         Up
GigabitEthernet0/0/0/3     unassigned                    Shutdown   Down
GigabitEthernet0/0/0/4     unassigned                    Shutdown   Down
```

This is the sample output of the **show ipv6 interface brief global** command:

```
RP/0/0/CPU0:router#show ipv6 interface brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     2001:db8::1                   Up         Up
GigabitEthernet0/0/0/1     2001:db8::2                   Up         Up
GigabitEthernet0/0/0/3     unassigned                    Shutdown   Down
GigabitEthernet0/0/0/4     unassigned                    Shutdown   Down
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 interface gigabitEthernet 0/0/0/0 brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     fe80::fe:8ff:fecb:26c5        Up         Up
```

This is the sample output of the **show ipv6 interface** *type interface-path-id* **brief global** command:

```
RP/0/0/CPU0:router#show ipv6 interface gigabitEthernet 0/0/0/0 brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/0     2001:db8::1                   Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     fe80::46:c8ff:fe22:daae       Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface brief global** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     2001:db8::2                   Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface** *type interface-path-id* **brief link-local** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief link-local

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     fe80::46:c8ff:fe22:daae       Up         Up
```

This is the sample output of the **show ipv6 vrf** *vrf-name* **interface** *type interface-path-id* **brief global** command:

```
RP/0/0/CPU0:router#show ipv6 vrf vrf1 interface gigabitEthernet 0/0/0/2 brief global

Interface                  IPv6-Address                  Status     Protocol
GigabitEthernet0/0/0/2     2001:db8::2                  Up         Up
```

Related Commands

Command	Description
show ipv4 interface , on page 72	Displays the usability status of interfaces configured for IPv4.

show ipv6 neighbors

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in the EXEC mode.

show ipv6 neighbors [*type interface-path-id*| **location** *node-id*]

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface instance or a virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

location *node-id*	(Optional) Designates a node. The *node-id* argument is entered in the *rack/slot/module* notation.

Command Default

All IPv6 neighbor discovery cache information is displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

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

When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Task ID

Task ID	Operations
ipv6	read

This is the sample output of the **show ipv6 neighbors** command when entered with an interface type and number:

```
RP/0/0/CPU0:router# show ipv6 neighbors POS 0/0/0/0

IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH POS2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH POS2
3001:1::45a                                 - 0002.7d1a.9472  REACH POS2
```

This is the sample output of the **show ipv6 neighbors** command when entered with an IPv6 address:

```
RP/0/0/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
```

This table describes significant fields shown in the display.

Table 13: show ipv6 neighbors Command Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.

Field	Description
State	

Field	Description
	The state of the neighbor cache entry. These are the states for dynamic entries in the IPv6 neighbor discovery cache: • INCMP (incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • reach (reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in reach state, the device takes no special action as packets are sent. • stale—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in stale state, the device takes no action until a packet is sent. • delay—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the delay state, send a neighbor solicitation message and change the state to probe. • probe—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. These are the possible states for static entries in the IPv6 neighbor discovery cache: • reach (reachable)—The interface for this entry is up. • INCMP (incomplete)—The interface for this entry is down. **Note** Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache;

Field	Description
	therefore, the descriptions for the INCMP (incomplete) and reach (reachable) states are different for dynamic and static cache entries.
Interface	Interface from which the address is reachable.

Related Commands

Command	Description
show ipv6 neighbors summary , on page 93	Displays summary information for the neighbor entries.

show ipv6 neighbors summary

To display summary information for the neighbor entries, use the **show ipv6 neighbors summary** command in the EXEC mode.

show ipv6 neighbors summary

Syntax Description This command has no keywords or arguments.

Command Default The default value is disabled.

Command Modes EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

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

Task ID

Task ID	Operations
ipv6	read

This is the sample output of the **show ipv6 neighbors summary** command that shows the summary information for the neighbor entries:

```
RP/0/0/CPU0:router# show ipv6 neighbors summary

Mcast nbr entries:
    Subtotal: 0
Static nbr entries:
    Subtotal: 0
Dynamic nbr entries:
    Subtotal: 0

Total nbr entries: 0
```

Related Commands

Command	Description
show ipv6 neighbors , on page 88	Displays IPv6 neighbor discovery cache information.

show ipv6 traffic

To display the IPv6 traffic statistics, use the **show traffic** command in the EXEC mode.

show ipv6 traffic [brief]

Syntax Description

brief	(Optional) Displays only IPv6 and Internet Control Message Protocol version 6 (ICMPv6) traffic statistics.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	Sample output was modified to display drop counters from the sanity address check.

Usage Guidelines

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

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

Task ID

Task ID	Operations
ipv6	read
network	read

This is the sample output of the **show ipv6 traffic** command:

```
RP/0/0/CPU0:router# show ipv6 traffic

 IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 reassembly max drop
         0  sanity address check drops
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor,
                 0 address, 0 port, 0 unknown
        parameter: 0 error, 0 header, 0 option,
                   0 unknown
        0 hopcount expired, 0 reassembly timeout,
        0 unknown timeout, 0 too big,
        0 echo request, 0 echo reply
  Sent: 0 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor,
                 0 address, 0 port, 0 unknown
        parameter: 0 error, 0 header, 0 option
                 0 unknown
        0 hopcount expired, 0 reassembly timeout,
        0 unknown timeout, 0 too big,
        0 echo request, 0 echo reply

Neighbor Discovery ICMP statistics:
  Rcvd: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert
  Sent: 0 router solicit, 0 router advert, 0 redirect
        0 neighbor solicit, 0 neighbor advert

UDP statistics:
        0 packets input, 0 checksum errors
        0 length errors, 0 no port, 0 dropped
        0 packets output
```

```
TCP statistics:s
        0 packets input, 0 checksum errors, 0 dropped
        0 packets output, 0 retransmitted
```

This table describes the significant fields shown in the display.

Table 14: show ipv6 traffic Command Field Descriptions

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

Related Commands

Command	Description
show ipv4 traffic , on page 77	Displays statistics about IPv4 traffic.

show mpa client

To display information about the Multicast Port Arbitrator (MPA) clients, use the **show mpa client** command in EXEC mode.

show mpa client {**consumers**| **producers**}

Syntax Description

consumers	Displays the clients for the consumers.
producers	Displays the clients for the producers.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read

The following sample output is from the **show mpa client** command:

```
RP/0/0/CPU0:router# show mpa client producers

List of producer clients for ipv4 MPA

Location     Protocol     Process
0/1/CPU0     255          raw
0/1/CPU0     17           udp
0/4/CPU0     17           udp
0/4/CPU0     255          raw
0/4/CPU1     17           udp
0/4/CPU1     255          raw
0/6/CPU0     17           udp
0/6/CPU0     255          raw
0/RP1/CPU0   17           udp
```

```
0/RP1/CPU0   255          raw
```

This table describes the significant fields shown in the display.

Table 15: show mpa client Command Field Descriptions

Field	Description
List of producer clients for MPA	Displays the producer clients that have registered with MPA.
Location	Displays the node on which the producer client is hosted.
Protocol	Displays the IP protocol ID.
Process	Displays the name of the producer client.

show mpa groups

To display Multicast Port Arbitrator (MPA) multicast group information, use the **show mpa groups** command in EXEC mode.

show mpa groups *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

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

Task ID

Task ID	Operations
network	read

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

```
RP/0/0/CPU0:router# show mpa groups gig 0/1/0/2
Mon Jul 27 04:07:19.802 DST
GigabitEthernet0/1/0/2 :-
  224.0.0.1 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.2 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.5 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.6 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.13 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.22 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
```

This table describes the significant fields shown in the display.

Table 16: show mpa groups Command Field Descriptions

Field	Description
Includes	Displays the number of client registrations that have enabled the group in the include mode.
Excludes	Displays the number of client registrations that have enabled the group in the exclude mode.
Mode	Displays the current mode for the address.

Field	Description
No source filter	Indicates that the router does not have the desired list of IP addresses.

Note The source filter consists of a list of source IP addresses. Depending on the mode, the list identifies the set of addresses from where multicast packets are either allowed or disallowed. In the include mode, the router accepts packets only from the IP addresses that are present in the source filter. In the exclude mode, the router drops packets from addresses that are present in the source filter. No source filter indicates that the registration does not have such a filter.

show mpa ipv4

To display information for Multicast Port Arbitrator (MPA) for IPv4, use the **show mpa ipv4** command in EXEC mode.

show mpa ipv4 {**client** {**consumers**| **producers**}| **groups** *type interface-path-id* }

Syntax Description

client	Displays information about the MPA clients.
consumers	Displays the clients for the consumers.
producers	Displays the clients for the producers.
groups	Displays information about the MPA multicast group.
type	Interface type. For more information, use the question mark (?) online help function.

interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read

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

```
RP/0/0/CPU0:router# show mpa ipv4 client producers

List of producer clients for ipv4 MPA

 Location     Protocol     Process
```

```
0/1/CPU0      17           udp
0/1/CPU0      255          raw
0/4/CPU0      17           udp
0/4/CPU0      255          raw
0/4/CPU1      17           udp
0/4/CPU1      255          raw
0/6/CPU0      17           udp
0/6/CPU0      255          raw
0/RP0/CPU0    17           udp
0/RP0/CPU0    255          raw
0/RP1/CPU0    255          raw
0/RP1/CPU0    17           udp
```

This table describes the significant fields shown in the display.

Table 17: show mpa ipv4 Command Field Descriptions

Field	Description
List of producer clients for ipv4 MPA	Displays the producer clients that have registered with MPA.
Location	Displays the node on which the producer client is hosted.
Protocol	Displays the IP protocol ID.
Process	Displays the name of the producer client.

show mpa ipv6

To display information for Multicast Port Arbitrator (MPA) for IPv6, use the **show mpa ipv6** command in EXEC mode.

show mpa ipv6 {**client** {**consumers**| **producers**}| **groups** *type interface-path-id*}

Syntax Description

client	Displays information about the MPA clients.
consumers	Displays the clients for the consumers.
producers	Displays the clients for the producers.
groups	Displays information about the MPA multicast group.
type	Interface type. For more information, use the question mark (?) online help function.

interface-path-id	Either a physical interface instance or a virtual interface instance as follows: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. ◦ *rack*: Chassis number of the rack. ◦ *slot*: Physical slot number of the modular services card or line card. ◦ *module*: Module number. A physical layer interface module (PLIM) is always 0. ◦ *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/ RP1/CPU0/0. • Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read

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

```
RP/0/0/CPU0:router# show mpa ipv6 client producers

List of producer clients for ipv6 MPA

 Location     Protocol     Process
```

```
0/1/CPU0      17           udp
0/1/CPU0      255          raw
0/4/CPU0      255          raw
0/4/CPU0      17           udp
0/4/CPU1      17           udp
0/4/CPU1      255          raw
0/6/CPU0      17           udp
0/6/CPU0      255          raw
0/RP0/CPU0    17           udp
0/RP0/CPU0    255          raw
0/RP1/CPU0    17           udp
0/RP1/CPU0    255          raw
```

Table 18: show mpa ipv6 Command Field Descriptions

Field	Description
List of producer clients for ipv6 MPA	Displays the producer clients that have registered with MPA.
Location	Displays the node on which the producer client is hosted.
Protocol	Displays the IP protocol ID.
Process	Displays the name of the producer client.

show svd role

To display selective VRF download feature role information, use the **show svd role** command in EXEC mode.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Example

This is a sample output from the **show svd role** command:

```
RP/0/0/CPU0:router# show svd role

Codes: (C) : user Configured role
Node Name       IPv4 Role                IPv6 Role
-----------------------------------------------------------------------
0/0/CPU0        Standard                 Standard
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

show vrf

To display the contents of the VPN routing and forwarding (VRF) instance, use the **show vrf** command in EXEC mode.

show vrf {**all**| *vrf-name*}

Syntax Description

all	Displays contents of all the VRFs.
vrf-name	Name that uniquely identifies the VRF.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
network	read, write

The following example shows how to use the **show vrf** command:

```
RP/0/0/CPU0:router# show vrf all

VRF                  RD                  RT                          AFI   SAFI
vpn_1                not set
                                         import  2:2                  IPV4  Unicast
                                         export  2:2                  IPV4  Unicast
vpn_2                not set
                                         import  3:3                  IPV4  Unicast
                                         export  3:3                  IPV4  Unicast
```

This table describes the significant fields shown in the display.

Table 19: show vrf Command Field Descriptions

Field	Description
VRF	User-assigned VRF names.
RD	Displays the associated route-distinguishers for each VRF.
RT	Displays import and export route target extended communities.
AFI	Displays the IP address family.
SAFI	Displays the VRF topology.

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

show vrf-group

To display all vrfs in a vrf group, use the **show vrf-group** command in EXEC mode.

show vrf-group *group-name* **location** *location*

Syntax Description

group-name	vrf-group with specified group-name
location *location*	vrfs corresponding to a specified location.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operation
ip-services	read

Example

This is a sample output from the **show vrf-group** command:

```
RP/0/0/CPU0:router# show vrf-group group1 location 0/0/CPU0
VRF-group : group1
Status    : Inactive
VRF count : 2
VRFs      :
   vrf1
   vrf2
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

vrf

To configure a VPN routing and forwarding (VRF) instance for a routing protocol, use the **vrf** command in router configuration mode. To disable the VRF instance, use the **no** form of this command.

vrf *vrf-name*

no vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF instance. The following names cannot be used: all, default, and global.

Command Default

All routing protocols insert their routes into a VRF's routing table.

Note The number of supported VRFs is platform specific.

Command Modes

Router configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ip services	read, write

The following example shows how to configure VRF using the **vrf** command:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# vrf client
```

vrf(address-family)

To configure the address family for a VRF instance, use the **vrf(address-family)** command in VRF configuration mode. To disable the address family, use the **no** form of this command.

vrf *vrf-name* [**address-family** {**ipv4**| **ipv6**} **unicast**]

no vrf *vrf-name* [**address-family** {**ipv4**| **ipv6**} **unicast**]

Syntax Description

vrf-name	Name of the VRF instance.
address-family	(Optional) Enables AFI or SAFI configuration.
ipv4	Enables address-family configuration for IPv4 addresses.
ipv6	Enables address-family configuration for IPv6 addresses.
unicast	Indicates unicast topology.

Command Default

None

Command Modes

VRF configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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

Task ID

Task ID	Operations
ip services	read, write

The following example shows how to configure the address family for a VRF instance, using the **vrf (address-family)** command:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# vrf client
RP/0/0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/0/CPU0:router(config-vrf-af)#
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

vrf-group

To configure a vrf-group, use the **vrf-group** command in global configuration mode. To deconfigure a vrf-group, use the **no** form of this command.

vrf-group *group-name* **vrf** *vrf-name*

no vrf-group *group-name* **vrf** *vrf-name*

Syntax Description

group-name	vrf-group with specified group-name.
vrf *vrf-name*	Creates a vrf under the specified vrf group.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Release 4.3.2	This command was introduced.

Usage Guidelines

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

The maximum vrf groups supported for a line card is 30. The maximum vrfs supported for each vrf-group is 300.

Task ID

Task ID	Operation
ip-services	read, write

Example

This example shows how to configure a vrf-group using the **vrf-group** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# vrf-group VRF1
RP/0/0/CPU0:router(config-vrf-group)# vrf vrf5
RP/0/0/CPU0:router(config-vrf-group)# vrf vrf6
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

vrf (description)

To add a brief description for the VRF instance being configured, use the **vrf (description)** command in VRF configuration mode. To remove a description, use the **no** form of this command.

vrf *vrf-name* **[description]**

no vrf *vrf-name* **[description]**

Syntax Description

vrf-name	Name of the VRF instance.
description	(Optional) Specifies a description for the VRF instance.

Command Default

No default behavior of values

Command Modes

VRF configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

Usage Guidelines

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

The description line can have a maximum of 244 characters.

Task ID

Task ID	Operations
ip services	read, write

The following example shows how to insert a description to a VRF instance using the **vrf (description)** command:

```
RP/0/0/CPU0:router# config
RP/0/0/CPU0:router(config)# vrf v1
RP/0/0/CPU0:router(config-vrf)# description client
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.

vrf (mhost)

To configure a multicast default interface for a particular VRF to send and receive packets from the host stack, use the **vrf (mhost)** command in VRF configuration mode. To remove the configuration, use the**no** form of this command.

vrf *vrf-name* [**mhost** {**ipv4**| **ipv6**} **interface**]

no vrf *vrf-name* [**mhost** {**ipv4**| **ipv6**} **interface**]

Syntax Description

vrf-name	Name of the VRF instance.
mhost	(Optional) Enables the multicast host stack options.
ipv4	Specifies IPv4 address.
ipv6	Specifies IPv6 address.
interface	Specifies the default *multicast interface.*

Command Default None

Command Modes VRF configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced.

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

The default interface should belong to the vrf for which its being configured.

Task ID

Task ID	Operations
ip services	read, write

The following example shows how to configure VRF a multicast default interface using the **vrf(mhost)** command:

```
RP/0/0/CPU0:router(config)# configvrf 101
RP/0/0/CPU0:router(config-vrf)# vrf clientmhost ipv4 default-interface loop101
```

Related Commands

Command	Description
vrf, on page 108	Configures a VRF instance for a routing protocol.