Cisco IOS IPv6 Command Reference

First Published: 2019-12-13

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

CONTENTS

IPv6 Commands: a to clear ipv6 mld

aaa accounting multicast default

To enable authentication, authorization, and accounting (AAA) accounting of IPv6 multicast services for billing or security purposes when you use RADIUS, use the **aaa accounting multicast default**command in global configuration mode. To disable AAA accounting for IPv6 multicast services, use the **no** form of this command.

aaa accounting multicast default [{**start-stop** | **stop-only**}] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*]
no aaa accounting multicast default [{**start-stop** | **stop-only**}] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*]

Syntax Description

start-stop	(Optional) Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
stop-only	(Optional) Sends a "stop" accounting notice at the end of the requested user process.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
method1 , *method2*, *method3*, *method4*	(Optional) Method lists that specify an accounting method or multiple accounting methods to be used for accounting.

Command Default

AAA accounting for multicast is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Note Including information about IPv6 addresses in accounting and authorization records transmitted between the router and the RADIUS or TACACS+ server is supported. However, there is no support for using IPv6 to communicate with that server. The server must have an IPv4 address.

Use the **aaa accounting multicast default**command to enable AAA accounting for multicast. The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. When using the **aaa accounting multicast default** command, you have the option of choosing one or all four existing named access lists, each of which specifies a RADIUS host or server group.

If the **aaa accounting multicast default**command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

For minimal accounting, include the **stop-only** keyword to send a "stop" record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process. Accounting is stored only on the RADIUS.

When AAA accounting is activated, the network access server monitors RADIUS accounting attributes pertinent to the connection. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix "RADIUS Attributes" in the *CiscoIOS Security Configuration Guide* .

Examples

The following example enables AAA accounting of IPv6 multicast services for billing or security purposes when RADIUS is used:

```
Router(config)# aaa accounting multicast default
```

Related Commands

Command	Description
aaa authorization multicast default	Sets parameters that restrict user access to an IPv6 network.

aaa accounting send counters ipv6

To send IPv6 counters in the stop record to the accounting server, use the **aaa accounting send counters ipv6**command in global configuration mode. To stop sending IPv6 counters, use the **no** form of this command.

aaa accounting send counters ipv6
no aaa accounting send counters ipv6

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 counters in the stop records are not sent to the accounting server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **aaa accounting send counters ipv6**command sends IPv6 counters in the stop record to the accounting server.

Examples

The following example shows how enable the router to send IPv6 counters in the stop record to the accounting server:

```
Router(config)# aaa accounting send counters ipv6
```

aaa authorization multicast default

To enable authentication, authorization, and accounting (AAA) authorization and set parameters that restrict user access to an IPv6 multicast network, use the **aaa authorization multicast default**command in global configuration mode. To disable authorization for a function, use the **no** form of this command.

aaa authorization multicast default [*method*]
no aaa authorization multicast default [*method*]

Syntax Description

method3 , *method4*	(Optional) Specifies one or two authorization methods that can be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Note Including information about IPv6 addresses in accounting and authorization records transmitted between the router and the RADIUS or TACACS+ server is supported. However, there is no support for using IPv6 to communicate with that server. The server must have an IPv4 address.

Use the **aaa authorization multicast default**command to enable authorization. Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is a named list describing the authorization methods to be used, in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS IPv6 software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS IPv6 software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS IPv6 software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or local username database responds by denying the user services--the authorization process stops, and no other authorization methods are attempted.

If the **aaa authorization multicast default** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all lines or interfaces (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Note In the table below, the **group radius** and **group***group-name* methods refer to a set of previously defined RADIUS servers. Use the **radius-server host**command to configure the host servers. Use the **aaa group server radius** command to create a named group of servers.

Method keywords are described in the table below.

Table 1: aaa authorization Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.
group *group-name*	Uses a subset of RADIUS servers for accounting as defined by the **server** group group-name command.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
local	Uses the local database for authorization.
none	No authorization is performed.

Cisco IOS IPv6 software supports the following methods for authorization:

- RADIUS--The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- If-Authenticated--The user is allowed to access the requested function provided the user has been authenticated successfully.
- None--The network access server does not request authorization information; authorization is not performed over this line or interface.
- Local--The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.

Method lists are specific to the type of authorization being requested. AAA supports the following different types of authorization:

- Network--Applies to network connections. This can include a PPP, Serial Line Internet Protocol (SLIP), or AppleTalk Remote Access (ARA) connection.
- EXEC--Applies to the attributes associated with a user EXEC terminal session.
- Commands--Applies to the EXEC mode commands and user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- Reverse Access--Applies to reverse Telnet sessions.

- Configuration--Applies to the configuration downloaded from the AAA server.

The **authorization** command causes a request packet containing a series of AV pairs to be sent to the RADIUS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and refuse authorization.

For a list of supported RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *CiscoIOS Security Configuration Guide* .

Examples

The following example enables AAA authorization and sets default parameters that restrict user access to an IPv6 multicast network:

```
Router(config)# aaa authorization multicast default
```

Related Commands

Command	Description
aaa accounting multicast default	Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
radius-server host	Specifies a RADIUS server host.
username	Establishes a username-based authentication system.

accounting (DHCP for IPv6)

To enable sending of accounting start and stop messages, use the **accounting** command in DHCP for IPv6 pool configuration mode. To remove configuration for these messages, use the **no** form of this command.

accounting *mlist*
no accounting *mlist*

Syntax Description

mlist	Accounting list to which start and stop messages are sent.

Command Default

Accounting start and stop messages are not configured.

Command Modes

DHCP for IPv6 pool configuration (config-dhcp)

Command History

Release	Modification
Cisco IOS Release XE 2.5	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **accounting** command allows users to configure and send accounting start and stop messages to a named accounting list. When accounting is configured for a DHCPv6 pool, accounting interim packets are sent to broadband sessions after binding is provided from the pool.

Examples

The following example configures accounting start and stop messages to be sent to an accounting list called list1:

```
Router(config)# ipv6 dhcp pool pool1
Router(config-dhcp)# accounting list1
```

address (Mobile IPv6)

To specify the home address of the IPv6 mobile node, use the **address**command in home-agent configuration mode or IPv6 mobile router host configuration mode. To remove a host configuration, use the **no** form of this command.

address {*ipv6-address* | **autoconfig**}
no address

Syntax Description

ipv6-address	Specifies a home address for the mobile node. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
autoconfig	Allows any IPv6 address to be used.

Command Default

No home address is specified for the mobile router.

Command Modes

Home-agent configuration (config-ha)
IPv6 mobile router host configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(20)T	IPv6 network mobility (NEMO) functionality was added.

Usage Guidelines

The **address** command in IPv6 home-agent configuration mode specifies the home address of the mobile node. The *ipv6-address*argument can be used to configure a specific IPv6 address, or the **autoconfig** keyword can be used to allow any IPv6 address as the home address of the IPv6 mobile node.

Do not configure two separate groups with the same IPv6 address. For example, host group group1 and host group group2 cannot both have the same home address of baba::1.

When the **address** command is configured with a specific IPv6 address, the **nai** command, which configures the network address identifier (NAI), cannot be configured using the *@realm* argument. For example, the following **nai** command configuration would not be valid because the **address** command is configured with the specific address baba::1:

```
host group engineering
  nai  @cisco.com
  address baba::1
```

Examples

In the following example, the user enters home agent configuration mode, creates a host group named group1, and configures any IPv6 address to be used for the mobile node:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)# host group group1
Router(config-ha)# address autoconfig
```

Related Commands

Command	Description
host group	Creates a host configuration in IPv6 Mobile.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

address ipv6 (TACACS+)

To configure the IPv6 address of the TACACS+ server, use the **address ipv6** command in TACACS+ server configuration mode. To remove the IPv6 address, use the **no** form of this command.

address ipv6 *ipv6-address*
no address ipv6 *ipv6-address*

Syntax Description

ipv6-address	The private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the address ipv6 (TACACS+) command after you have enabled the TACACS+ server using the **tacacs server** command.

Examples

The following example shows how to specify the IPv6 address on a TACACS+ server named server1:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

address prefix ipv6-prefix [**lifetime** {**valid-lifetime preferred-lifetime** | **infinite**}]
no address prefix

Syntax Description

ipv6-prefix	IPv6 address prefix.
lifetime {valid-lifetime preferred-lifetime | infinite}]	(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the **infinite** keyword is specified, the time interval does not expire.

Command Default

No IPv6 address prefix is assigned.

Command Modes

DHCP pool configuration (config-dhcpv6)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

You can use the **address prefix** command to configure one or several address prefixes in an IPv6 DHCP pool configuration. Each time the IPv6 DHCP address pool is used, an address will be allocated from each of the address prefixes associated with the IPv6 DHCP pool.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

address-family ipv4 (OSPFv3)

To enter IPv4 address family configuration mode for Open Shortest Path First version 3 (OSPFv3), use the address-family ipv4 command in OSPFv3 router configuration mode.

address-family ipv4 unicast[**vrf** *vrf-name*]

Syntax Description

unicast	Specifies IPv4 unicast address prefixes.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

This command is disabled by default.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **address-family ipv4** command to configure the IPv4 address family in the OSPFv3 process. Only one address family can be configured per instance. Several IPv4 address family-specific commands are available once you have enabled the **address-family ipv4** command and entered IPv4 address family configuration mode.

Examples

The following example enters IPv4 address family configuration mode for OSPFv3:

```
Router(config-router)#address-family ipv4 unicast
Router(config-router-af)#
```

Related Commands

router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

address-family ipv6

To enter address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv6 [{**unicast** | **multicast** | **vpnv6**}] [{**vrf** *vrf-name*}]
no address-family ipv6 [{**unicast** | **multicast** | **vpnv6**}] [{**vrf** *vrf-name*}]

Syntax Description

unicast	(Optional) Specifies IPv6 unicast address prefixes.
multicast	(Optional) Specifies IPv6 multicast address prefixes.
vpnv6	(Optional) Specifies VPN Version 6 address prefixes.
vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for an IPv6 address.
vrf-name	(Optional) A specific VRF table for an IPv6 address.

Command Default

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(26)S	The **multicast** keyword was added.
12.3(4)T	The **multicast** keyword was added.
12.2(25)S	The **multicast** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	The **vpnv6** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.6S	The **mvpn** keyword was added.
Cisco IOS XE Release 3.7S	The **multicast** keyword was added.
15.2(4)S	The **multicast** keyword was added.
15.2(S)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(4)M	This command was modified. The **mvpn** keyword was added.

Usage Guidelines

The **address-family ipv6** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use standard IPv6 address prefixes.

The BGP commands supported in address family configuration mode configure the same functionality as the BGP commands supported in router configuration mode; however, the BGP commands in router configuration mode configure functionality only for the IPv4 unicast address prefix. To configure BGP commands and functionality for other address family prefixes (for example, the IPv4 multicast or IPv6 unicast address prefixes), you must enter address family configuration mode for those address prefixes using the **address-family ipv4** command or the **address-family ipv6** command.

Use the **multicast** keyword to specify an administrative distance for multicast BGP routes to be used in reverse path forwarding (RPF) lookups.

Examples

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)#
```

The following example places the router in address family configuration mode and specifies multicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv6 multicast
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

address-family ipv6 (IS-IS)

To enter address family configuration mode for configuring Intermediate System-to-Intermediate System (IS-IS) routing sessions that use standard IPv6 address prefixes, use the address-family ipv6 command in router configuration mode. To reset all IPv6-specific global configuration values to their default values, use the **no** form of this command.

address-family ipv6 [**unicast**]
no address-family ipv6 [**unicast**]

Syntax Description

unicast	(Optional) Specifies IPv6 unicast address prefixes.

Command Default

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Command Modes

Router configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

The **address-family ipv6** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure IPv6-specific settings. To leave address family configuration mode and return to router configuration mode, enter the **exit-address-family**command.

Within address family configuration mode, use the question mark (?) online help function to display supported commands. Many of the IS-IS commands supported in address family configuration mode are identical in syntax to IS-IS commands supported in router configuration mode. Note that commands issued in address family configuration mode apply to IPv6 only, while the matching commands in router configuration mode are IPv4-specific.

Examples

The following example places the router in address family configuration mode for IS-IS and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6 unicast
```

address-family ipv6 (OSPFv3)

To enter IPv6 address family configuration mode for Open Shortest Path First version 3 (OSPFv3), use the **address-family ipv6** command in OSPFv3 router configuration mode.

address-family ipv6 **[unicast]** [**vrf** *vrf-name*]

Syntax Description

unicast	(Optional) Specifies IPv6 unicast address prefixes.
vrf *vrf-name*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

None

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was modified. Support for nonstop routing (NSR) in address family configuration mode was added.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **address-family ipv6** command to configure the IPv6 address family in the OSPFv3 process. Only one address family can be configured per instance. Several IPv6 address family-specific commands are available once you have enabled the **address-family ipv6** command and entered IPv6 address family configuration mode.

When an NSR subsystem is included in an image and OSPFv3 NSR is supported on both the active and standby Route Processors (RPs), you can use the **nsr** command in address family configuration mode to enable NSR or to disable it for a specific address family.

Examples

The following example enters IPv6 address family configuration mode for OSPFv3:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)#
```

Related Commands

nsr (OSPFv3)	Enables or disables NSR operations on a router that is running OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

address-family vpnv6

To place the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes, use the **address-family vpnv6** command in router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family vpnv6 [{**unicast** | **multicast**}]
no address-family vpnv6 [{**unicast** | **multicast**}]

Syntax Description

unicast	(Optional) Specifies VPN Version 6 unicast address prefixes.
multicast	(Optional) Specifies VPN Version 6 multicast address prefixes.

Command Default

VPN Version 6 address prefixes are not enabled. Unicast address prefixes are the default when VPN Version 6 address prefixes are configured.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.7S	The **multicast** keyword was added.
15.2(4)S	The **multicast** keyword was added.
15.2(S)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **address-family vpnv6** command places the router in address family configuration mode, from which you can configure routing sessions that use VPN Version 6 address prefixes. An address family must be configured for each VPN routing/forwarding (VRF) on a provider edge (PE) router. Furthermore, a separate address family must be configured for carrying VPN-IPv6 routes between PE routers.

Examples

The following example places the router in address family configuration mode for the VPN Version 6 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family vpnv6
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a BGP neighbor.

adjacency-check

To allow Intermediate System-to-Intermediate System (IS-IS) IPv6 or IPv4 protocol-support consistency checks performed on hello packets, use the **adjacency-check** command in address family configuration or router configuration mode. To disable consistency checks on hello packets, use the **no** form of this command.

adjacency-check
no adjacency-check

Syntax Description

This command has no arguments or keywords.

Command Default

The feature is enabled.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	Support was added for router configuration mode.
12.2(18)S	Support was added for router configuration mode.
12.0(26)S	Support was added for router configuration mode.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

IS-IS performs consistency checks on hello packets and will form an adjacency only with a neighboring router that supports the same set of protocols. A router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 only.

Use the **no adjacency-check** command in address-family configuration mode to suppress the consistency checks for IPv6 IS-IS and allow an IPv4 IS-IS router to form an adjacency with a router running IPv4 IS-IS and IPv6. IS-IS will never form an adjacency between a router running IPv4 IS-IS only and a router running IPv6 only.

Use the **no adjacency-check** command in router configuration mode to suppress the IPv4 subnet consistency check and allow IS-IS to form an adjacency with other routers regardless of whether or not they have an IPv4 subnet in common. By default, IS-IS makes checks in hello packets for IPv4 address subnet matching with a neighbor. In multitopology mode, the IPv4 subnet consistency check is automatically suppressed.

Tip Use the **debug isis adjacency packets** command in privileged EXEC mode to check for adjacency errors. Error messages in the output may indicate where routers are failing to establish adjacencies.

Examples

In the following example, the network administrator wants to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, the network administrator enters the **no adjacency-check** command.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# no adjacency-check
```

In IPv4, the following example shows that the network administrator wants to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, the network administrator enters the **no adjacency-check** command.

```
Router(config)# router isis
Router(config-router-af)# no adjacency-check
```

advertise passive-only (IPv6)

To configure Intermediate System-to-Intermediate System (IS-IS) to advertise only IPv6 prefixes that belong to passive interfaces, use the **advertise passive-only** command in address family configuration mode. To remove the restriction, use the **no** form of this command.

advertise passive-only
no advertise passive-only

Syntax Description

This command has no arguments or keywords.

Command Default

IS-IS does not advertise only IPv6 prefixes that belong to passive interfaces.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

This command is an IS-IS mechanism to exclude IPv6 prefixes of connected networks from link-state packet (LSP) advertisements, thereby reducing IS-IS convergence time.

Configuring this command per IS-IS instance is a scalable method to reduce IS-IS convergence time because fewer IPv6 prefixes will be advertised in the router nonpseudonode LSP.

This command relies on the fact that when enabling IS-IS on a loopback interface, you usually configure the loopback as passive (to prevent sending unnecessary hello packets out through it because there is no chance of finding a neighbor behind it). Thus, if you want to advertise only the loopback and if it has already been configured as passive, configuring the **advertise passive-only** command per IS-IS instance prevents overpopulation of the routing tables.

An alternative to this command is the **no isis advertise-prefix** command, which is a small-scale method because it is configured per interface.

Examples

The following example uses the **advertise passive-only** command, which affects the IS-IS instance, and thereby prevents advertising the IPv6 network of Gigabit Ethernet interface 0/0/0. Only the IPv6 address of loopback interface 0 is advertised.

```
router isis
 net 49.0000.0000.0100.00
 metric-style wide
 address-family ipv6
   advertise passive-only
   interface GigabitEthernet 0/0/0
    ipv6 address 2001::1/64
    ipv6 router isis
    interface loopback 0
    ipv6 address 2002::1/128
    router isis
```

```
  passive-interface loopback 0
  end
```

show isis database detail level-1

```
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
Device.00-00     * 0x00000004   0x8EB2        1192              0/0/0
  Area Address: 49
  NLPID:        0xCC 0x8E
  Hostname: Device
  IPv6 Address: 2002::1
  Metric: 0          IPv6 2002::1/128
```

Related Commands

Command	Description
address-family ipv6 (IS-IS)	Enters address family configuration mode for configuring IS-IS routing sessions that use standard IPv6 address prefixes.
isis advertise-prefix	Allows the advertising of IP prefixes of connected networks in LSP advertisements per IS-IS interface.
passive-interface	Suppresses the sending of routing updates through the specified interface.

area (IPv6 address family configuration)

To configure Open Shortest Path First version 3 (OSPFv3) area parameters, use the area command in IPv6 address family configuration mode or IPv4 address family configuration mode. To remove this configuration, use the **no** form of this command.

area *area-ID* **range** *ipv6-prefix/prefix-length*

Syntax Description

area-ID	Area ID associated with the OSPFv3 interface.
range	Summarizes routes that match the address or address mask on border routers only.
ipv6-prefix / *prefix-length*	An IPv6 prefix (address) and prefix length.
virtual-link	Defines a virtual link and its parameters. • This keyword can be used with the IPv6 address family only.
router-id	Router ID associated with the virtual-link neighbor. • This keyword can be used with the IPv6 address family only.

Command Default

This command is disabled by default.

Command Modes

IPv6 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **area**command in IPv6 or IPv4 address family configuration mode to configure OSPFv3 area parameters for an IPv6 or an IPv4 process.

Examples

The following example summarizes routes on the border router with the 2001:DB8:0:0::0/128 address:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.

Command	Description
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

area_(OSPFv3)

To configure the Open Shortest Path First version 3 (OSPFv3) area, use the area command in OSPFv3 router configuration mode. To remove this configuration, use the **no** form of this command.

area *area-ID* [{**default-cost** | **nssa** | **stub**}]

Syntax Description

default-cost	(Optional) Configures the cost for the default summary route used for a stub or not-so-stubby area (NSSA).
nssa	(Optional) Configures the NSSA.
stub	(Optional) Defines an area as a stub area.

Command Default

This command is not enabled by default.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **area** command in OSPFv3 router configuration mode to configure OSPFv3 parameters for an IPv4 OSPFv3 process.

Examples

The following example configures OSPFv3 area 1:

```
Router(config-router)# area 1
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

area authentication (IPv6)

To enable authentication for an Open Shortest Path First (OSPF) area, use the **area authentication** command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the **no** form of this command.

area *area-id* **authentication ipsec spi** *spi* *authentication-algorithm* [*key-encryption-type*] *key*
no area *area-id* **authentication ipsec spi** *spi*

Syntax Description

area-id	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
ipsec	Specifies IP Security (IPsec).
spi *spi*	Specifies the security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295, which is entered as a decimal.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5** —Enables message digest 5 (MD5) authentication. • **sha1** —Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	(Optional) Identifier of values that can be entered: • 0—The key is not encrypted. • 7—The key is encrypted.
key	Number used in the calculation of the message digest. The number is 32 hexadecimal digits (16 bytes) long.

Command Default

Key encryption type 0; that is, the key is not encrypted.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	The command was modifed. The **sha1** keyword was added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

Ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may be automatically used by other client applications, such as tunnels.

The policy database is common to all client applications on a device. This means that two IPsec clients, such as OSPF and a tunnel, cannot use the same SPI. Additionally, an SPI can only be used in one policy.

Beginning with Cisco IOS Release 12.4(4)T, the **sha-1** keyword can be used to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is considered to be somewhat more secure than the MD5 algorithm, and it requires a 40-hexadecimal-digit (20-byte) key rather than the 32-hexadecimal-digit (16-byte) key that is required for MD5 authentication.

Examples

The following example shows how to enable authentication for the OSPF area 1:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# area 1 authentication ipsec spi 678 md5
1234567890ABCDEF1234567890ABCDEF
```

The following example shows how to enable SHA-1 authentication for the OSPF area 0:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# area 0 authentication ipsec spi 1000 sha1
1234567890123456789012345678901234567890
```

Related Commands

Command	Description
area encryption	Enables encryption for an OSPF area.
area virtual-link authentication	Enables authentication for virtual links in an OSPF area.
area virtual-link encryption	Enables encryption for virtual links in an OSPF area.
ipv6 ospf authentication	Specifies the authentication type for an OSPF interface.

area range

To consolidate and summarize routes at an area boundary, use the **a rea range** command in router configuration mode. To disable this function, use the **no**form of this command.

area *area-id* **range** *ipv6-prefix* / *prefix-length* [{**advertise** | **not-advertise**}] [**cost** *cost*]
no area *area-id* **range** *ipv6-prefix* / *prefix-length* [{**advertise** | **not-advertise**}] [**cost** *cost*]

Syntax Description

area-id	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
ipv6-prefix	IPv6 prefix.
/ *prefix-length*	IPv6 prefix length.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
cost *cost*	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(24)S	Support for IPv6 was added. The **cost** keyword and *cost* argument were added.
12.2(15)T	Support for IPv6 was added. The **cost** keyword and *cost* argument were added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*

Multiple **area** router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

This command has been modified for Open Shortest Path First (OSPF) for IPv6. Users can now enter the IPv6 address syntax.

Note To remove the specified area from the software configuration, use the **no area** *area-id*command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface Ethernet0/0
 no ip address
 ipv6 enable
 ipv6 ospf 1 area 1
!
ipv6 router ospf 1
 router-id 192.168.255.5
 log-adjacency-changes
 area 1 range 2001:0DB8:0:1::/64
```

The following example shows the IPv6 address syntax:

```
Router(config-rtr)# area 1 range ?
 X:X:X:X::X/<0-128>  IPv6 prefix x:x::y/z
```

authentication (Mobile IPv6)

To specify the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional security parameter index (SPI), use the **authentication** command in home-agent configuration mode or IPv6 mobile router host configuration mode. To remove these authentication properties, use the **no** form of this command.

authentication {**inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**algorithm** *algorithm-type*] [**replay within** *seconds*]
no authentication

Syntax Description

inbound-spi	Bidirectional SPI used to authenticate inbound registration packets.
hex-in	Index for inbound registration packets. The range is from 100 to ffffffff.
decimal *decimal-in*	SPI expressed as a decimal number for inbound registration packets. The range is from 256 to 4294967295.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets.
hex-out	Index for outbound registration packets. The range is from 100 to ffffffff.
decimal *decimal-out*	SPI expressed as a decimal number. The range is from 256 to 4294967295.
spi	Unidirectional SPI used to authenticate a peer. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability.
hex-value	SPI expressed as a hexadecimal number. The range is from 100 to ffffffff.
decimal *decimal-value*	SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key.
ascii *string*	Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed.
hex *string*	Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
algorithm	(Optional) Algorithm used to authenticate messages during registration.
algorithm-type	(Optional) Type of algorithm. The hash-based Message Authentication Code (HMAC)-SHA1 algorithm is used.
replay within	(Optional) Specifies the number of seconds that the router uses for replay protection.

seconds	(Optional) Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.

Command Default

No SPI is configured.

Command Modes

Home-agent configuration (config-ha)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(20)T	IPv6 network mobility (NEMO) functionality was added.

Usage Guidelines

The **authentication** command provides mobility message authentication by creating a mobility SPI, a key, an authentication algorithm, and a replay protection mechanism. Mobility message authentication option is used to authenticate binding update (BU) and binding acknowledgment (BA) messages based on the shared-key-based security association between the mobile node and the home agent.

The mobile node or home agent receiving this BU must verify the authentication data in the option. If authentication fails, the home agent must send a FAIL message. If the home agent does not have shared-key-based mobility SA, the home agent MUST discard the BU.

The mobility message replay protection option may be used in BU or BA messages when authenticated using the mobility message authentication option. The mobility message replay protection option, configured using the **replay within** keywords, is used to let the home agent verify that a BU has been freshly generated by the mobile node and not replayed by an attacker from some previous BU. This function is especially useful for cases in which the home agent does not maintain stateful information about the mobile node after the binding entry has been removed. The home agent performs the replay protection check after the BU has been authenticated. The mobility message replay protection option, when included, is used by the mobile node for matching the BA with the BU.

Examples

The following example shows a unidirectional SPI and a key:

```
authentication spi 500 key ascii cisco
```

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 mobile node,
host group	Creates a host configuration in IPv6 Mobile.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

auto-cost (IPv6)

To control the reference value Open Shortest Path First (OSPF) for IPv6 uses when calculating metrics for interfaces, use the **auto-cost** command in router configuration mode. To return the reference value to its default, use the **no** form of this command.

auto-cost reference-bandwidth *Mbps*
no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *Mbps*	Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.

Command Default

The reference value is 100 Mbps.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The OSPF for IPv6 metric is calculated as the *Mbps*value divided by the bandwidth, with *Mbps*equal to 108 by default, and bandwidth determined by the **bandwidth** (interface) command. The calculation gives Fast Ethernet a metric of 1.

If you have multiple links with high bandwidth (such as Fast Ethernet or ATM), you might want to use a larger number to differentiate the cost on those links.

Using this formula, the default path costs were calculated as noted in the following bulleted list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link--Default cost is 1785.
- 64-kbps serial link--Default cost is 1562.
- T1 (1.544-Mbps serial link)--Default cost is 64.
- E1 (2.048-Mbps serial link)--Default cost is 48.
- 4-Mbps Token Ring--Default cost is 25.
- Ethernet--Default cost is 10.
- 16-Mbps Token Ring--Default cost is 6.
- Fast Ethernet--Default cost is 1.
- X25--Default cost is 5208.
- Asynchronous--Default cost is 10,000.
- ATM--Default cost is 1.

The value set by the **ipv6 ospf cost** command overrides the cost resulting from the **auto-cost** command.

Examples

The following example sets the auto-cost reference bandwidth to 1000 Mbps:

```
ipv6 router ospf 1
 auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
ipv6 ospf cost	Explicitly specifies the cost of sending an IPv6 packet on an interface.

auto-cost (OSPFv3)

To control the reference value Open Shortest Path First version 3 (OSPFv3) uses when calculating metrics for interfaces in an IPv4 OSPFv3 process, use the **auto-cost** command in OSPFv3 router configuration mode. To return the reference value to its default, use the **no** form of this command.

auto-cost reference-bandwidth *Mbps*
no auto-cost reference-bandwidth

Syntax Description

reference-bandwidth *Mbps*	Rate in Mbps (bandwidth). The range is from 1 to 4294967. The default is 100.

Command Default

The reference value is 100 Mbps.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The OSPF version 3 metric is calculated as the *Mbps*value divided by the bandwidth, with *Mbps*equal to 108 by default, and bandwidth determined by the **bandwidth** (interface) command. The calculation gives Fast Ethernet a metric of 1.

If you have multiple links with high bandwidth (such as Fast Ethernet or ATM), you might want to use a larger number to differentiate the cost on those links.

Using this formula, the default path costs were calculated as noted in the following bulleted list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link--Default cost is 1785.
- 64-kbps serial link--Default cost is 1562.
- T1 (1.544-Mbps serial link)--Default cost is 64.
- E1 (2.048-Mbps serial link)--Default cost is 48.
- 4-Mbps Token Ring--Default cost is 25.
- Ethernet--Default cost is 10.
- 16-Mbps Token Ring--Default cost is 6.
- Fast Ethernet--Default cost is 1.

- X25--Default cost is 5208.
- Asynchronous--Default cost is 10,000.
- ATM--Default cost is 1.

The value set by the **ospfv3 cost** or **ipv6 ospf cost** command overrides the cost resulting from the **auto-cost** command.

Examples

The following example sets the auto-cost reference bandwidth to 1000 Mbps:

```
router ospfv3 1
 auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
ipv6 ospf cost	Explicitly specifies the cost of sending an IPv6 packet on an interface.
ospfv3 cost	Explicitly specifies the cost of sending a packet on an OSPFv3 interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

bfd all-interfaces (OSPFv3)

To enable Bidirectional Forwarding Detection (BFD) for an Open Shortest Path First version 3 (OSPFv3) routing process, use the **bfd all-interfaces**command in OSPFv3 router configuration mode. To disable BFD for the OSPFv3 routing process, use the **no** form of this command.

bfd all-interfaces
no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is disabled on the interfaces participating in the routing process.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **bfd all-interfaces** command in OSPFv3 router configuration mode to enable BFD for all OSPFv3 interfaces.

Examples

The following example shows how to enable BFD for all Open Shortest Path First (OSPF) neighbors:

```
Router(config)# router ospfv3 123
Router(config-router)# bfd all-interfaces
Router(config-router)# end
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

bgp default ipv6-nexthop

To set the IPv6 unicast nex-thop format as the default for Border Gateway Protocol (BGP) IPv6 updates, use the **bgp default ipv6-nexthop** command in router configuration mode. To disable the default IPv6 unicast next-hop format as the default, use the **no** form of this command.

bgp default ipv6-nexthop
no bgp default ipv6-nexthop

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default and is not shown in the running configuration.

Command Modes

Router configuration

Command History

Release	Modification
12.0(32)SY9	This command was introduced.

Usage Guidelines

The **bgp default ipv6-nexthop** command enables BGP to choose the IPv6 next hop automatically for IPv6 address family prefixes.

Use the **no bgp default ipv6-nexthop** command to disable automatic next-hop selection in the following situations when IPv6 next-hop selection is configured to propogate over IPv4 sessions:

- If a route map is applied, then use the next hop given in the route map.
- If a route map is not configured, do one of the following:
  - If the router has directly connected peering configured, pick up a IPv6 address (both global and link-local IPv6 addresses)
  - If loopback peering is configured, pick up a IPv6 address from the loopback interface (both global and link-local IPv6 addresses)
  - The router configuration falls back to the default behavior of a IPv4-mapped IPv6 address.

Examples

The following example disables the unicast next-hop format for router process 50000:

```
Router(config)# router bgp 50000
Router(config-router)# no bgp default ipv6-nexthop
```

bgp recursion host

To enable the recursive-via-host flag for IP Version 4 (IPv4), VPN Version 4 (VPNv4), virtual routing and forwarding (VRF) address families, and IPv6 address families, use the **bgp recursion host** command in address family configuration or router configuration mode. To disable the recursive-via-host flag, use the **no** form of this command.

bgp recursion host
no bgp recursion host

Syntax Description

This command has no arguments or keywords.

Command Default

For an internal Border Gateway Protocol (iBGP) IPv4 address family, irrespective of whether Prefix Independent Convergence (PIC) is enabled, the recursive-via-host flag in Cisco Express Forwarding is not set.

For the VPNv4 and IPv4 VRF address families, the recursive-via-host flag is set and the **bgp recursion host** command is automatically restored when PIC is enabled under the following conditions:

- The **bgp additional-paths install** command is enabled.
- The **bgp advertise-best-external** command is enabled.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **bgp recursion host** command is used to help Cisco Express Forwarding during traffic route absence when a node failure occurs.

For link protection, BGP automatically restricts the recursion for the next hop resolution of connected routes. These routes are provided by the route reflector, which receives the prefix from another provider edge (PE) router that needs the customer edge (CE) router to be protected.

For node protection, BGP automatically restricts the recursion for the next hop resolution of host routes. These routes are provided by the route reflector, which receives the prefix from the host PE router. If a PE router or Autonomous System Boundary Router (ASBR) fails, for the **bgp recursion host** command to work, the PE routers must satisfy the following options:

- The host prefix must be used on the PE loopback interfaces.
- The next-hop-self must be configured on iBGP sessions.
- The **recursive via host prefix** command must be configured.

To enable Cisco Express Forwarding to use strict recursion rules for an IPv4 address family, you must configure the **bgp recursion host** command that enables the recursive-via-host flag when PIC is enabled.

The recursive-via-connected flag is set for directly connected peers only. For example, if the **bgp additional-paths install** command is configured in IPv4 and IPv4 VRF address family configuration modes, the running configuration shows the following details:

```
address-family ipv4
bgp additional-paths-install
no bgp recursion host
!
address-family ipv4 vrf red
bgp additional-paths-install
bgp recursion host
```

In the case of an external Border Gateway Protocol (eBGP) directly connected peers route exchange, the recursion is disabled for the connected routes. The recursive-via-connected flag is automatically set in the RIB and Cisco Express Forwarding for the routes from the eBGP single-hop peers.

For all the VPNs, irrespective of whether PIC is enabled, when the **bgp recursion host** command is configured in VPNv4 and IPv4 address family configuration modes, the normal recursion rules are disabled and only recursion via host-specific routes is allowed for primary, backup, and multipaths under those address families. To enable the normal recursion rules, configure the **no bgp recursion host** command in VPNv4 and IPv4 address family configuration modes.

Examples

The following example shows the configuration of the **bgp advertise-best-external** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
```

```
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp advertise-best-external
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family
```

The following example shows the configuration of the **bgp additional-paths install** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp additional-paths install
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family
```

The following example shows the best external routes and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 4
Paths: (2 available, best #2, table test1)
  Advertise-best-external
  Advertised to update-groups:
     1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
```

```
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

The following example shows the additional paths and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 25
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

The table below describes the significant fields shown in the display.

Table 2: show ip bgp vpnv4 vrf network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Advertised to update-groups	IP address of the BGP peers to which the specified route is advertised.
10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP--Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete--Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP--Entry originated from an EGP.
metric	The value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 50.

Field	Description
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is *internal* if the path is learned via iBGP. The field is *external* if the path is learned via eBGP.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.

binding

To configure binding options for the Mobile IPv6 home agent feature, use the **binding**command in home agent configuration mode. To restore parameters to default values, use the **no** form of this command.

binding [{**access** *access-list-nameauth-optionsecondsmaximumrefresh*}]
no binding [{**access** *access-list-nameauth-optionsecondsmaximumrefresh*}]

Syntax Description

access	(Optional) Specifies an access list to limit response.
access-list-name	(Optional) Access control list used to configure a binding update filter. When an access control list is configured, all Dynamic Home Agent Address Discovery (DHAAD) requests and binding updates are filtered by the home address and destination address.
auth-option	(Optional) Valid authentication option, which authenticates the binding update and binding acknowledgment messages based on the shared-key-based security association between the mobile node and the home agent.
seconds	(Optional) Permissible maximum binding lifetime, in number of seconds. The lifetime granted in the binding acknowledgment (binding ack) parameter is always the smallest of the requested lifetime, subnet lifetime, and configured permissible lifetime parameters.
maximum	(Optional) Maximum number of binding cache entries. If the value is set to 0, no new binding requests are accepted. Existing bindings are allowed to expire gracefully.
refresh	(Optional) Suggested binding refresh interval, in number of seconds. If the registration lifetime is greater than the configured binding refresh interval, this value is returned to the mobile node in the binding refresh advice option in the binding ack sent by the home agent.

Command Default

No access list is used to configure a binding update filter. The default value for the *seconds*argument is 262140, which is the maximum permissible binding time. The default value for the *maximum* argument is a number of entries limited by memory available on the router. The default value of the *refresh*argument is 300 sec.

Command Modes

Home agent configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	The *auth-option* argument was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you enable the **ipv6 mobile home-agent** command on an interface, you should configure common parameters on the router using the **binding** command. This command does not enable home agent service on the interfaces.

If the configured number of home agent registrations is reached or exceeded, subsequent registrations will be refused with the error "Insufficient resources." No existing bindings will discarded until their lifetime has expired, even if the *maximum* argument is set to a value lower than the current number of such bindings.

The appropriate value for the *refresh* argument will depend on whether the router is operating any high-availability features. If it is not, and a failure would cause the bindings cache to be lost, set the refresh argument to a low value.

Examples

In the following example, the maximum number of binding cache entries is set to 15:

```
binding 15
```

Related Commands

Command	Description
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

cdma pdsn ipv6

To enable the packet data serving node (PDSN) IPv6 functionality, use the cdma pdsn ipv6 command in global configuration mode. To disable this function, use the no form of the command.

cdma pdsn ipv6 ra-count ra-value [**ra-interval seconds**]
no cdma pdsn ipv6 ra-count ra-value [**ra-interval seconds**]

Syntax Description

ra-count	Routing advertisement (RA) count determines how many RAs to send to the MN.
ra-value	Number of IPv6 RAs to be sent. The range is from 1 to 5, and the default value is 1.
ra-interval	RA interval determines how often RAs are sent to the MN.
seconds	The interval between IPv6 RAs sent. The range is from 1 to 1800, and the default value is 5.

Command Default

Number of IPv6 RAs to be sent is 1. The interval between IPv6 RAs sent is 5 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)XY	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

If the cdma pdsn ipv6 command is not entered and a PDSN session is brought up with IPv6, the session will be terminated and the following message displayed:

%CDMA_PDSN-3-PDSNIPV6NOTENABLED: PDSN IPv6 feature has not been enabled.

Examples

The following example illustrates how to control the number and interval of routing advertisements sent to the MN when an IPv6 session comes up:

```
router(config)# cdma pdsn ipv6 ra-count 2 r
a-interval 3
```

clear bgp ipv6

To reset IPv6 Border Gateway Protocol (BGP) sessions, use the **clear bgp ipv6**command in privileged EXEC mode.

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
*	Resets all current BGP sessions.
autonomous-system-number	Resets BGP sessions for BGP neighbors within the specified autonomous system.
ip-address	Resets the TCP connection to the specified IPv4 BGP neighbor and removes all routes learned from the connection from the BGP table.
ipv6-address	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
peer-group-name	Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table.
soft	(Optional) Soft reset. Does not reset the session.
in **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft resets are triggered.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added to Cisco IOS Release 12.3(2)T.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast**keyword was added to Cisco IOS Release 12.3(4)T.

Release	Modification
12.2(25)S	The **multicast**keyword was added to Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **clear bgp ipv6**command is similar to the **clear ip bgp**command, except that it is IPv6-specific.

Use of the **clear bgp ipv6** command allows a reset of the neighbor sessions with varying degrees of severity depending on the specified keywords and arguments.

Use the **clear bgp ipv6 unicast** command to drop neighbor sessions with IPv6 unicast address prefixes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Use the **clear bgp ipv6 ***command to drop all neighbor sessions. The Cisco IOS software will then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use t he **clear bgp ipv6 soft out** or the **clear bgp ipv6 unicast soft out**command to drop only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Use the **clear bgp ipv6 soft in**or the **clear bgp ipv6 unicast soft in**command to drop only the inbound neighbor connections. Outbound neighbor sessions will not be reset. To reset inbound routing table updates dynamically for a neighbor, you must configure the neighbor to support the router refresh capability. To determine whether a BGP neighbor supports this capability, use the **show bgp ipv6 neighbors** or the **show bgp ipv6 unicast neighbors**command. If a neighbor supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If all BGP networking devices support the route refresh capability, use the **clear bgp ipv6** {*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in** or the **clear bgp ipv6 unicast**{*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in**command. Use of the **soft** keyword is not required when the route refresh capability is supported by all BGP networking devices, because the software automatically performs a soft reset.

Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Examples

The following example clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example uses the **unicast** keyword and clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example clears the outbound session with the peer group named marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast marketing soft out
```

The following example uses the **unicast** keyword and clears the outbound session with the peer group named peer-group marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast peer-group marketing soft out
```

Related Commands

Command	Description
show bgp ipv6	Displays entries in the IPv6 BGP routing table.

clear bgp ipv6 dampening

To clear IPv6 Border Gateway Protocol (BGP) route dampening information and unsuppress the suppressed routes, use the **clear bgp ipv6 dampening** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **dampening** [*ipv6-prefix* /*prefix-length*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) IPv6 network about which to clear dampening information. 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*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

When the *ipv6-prefix* / *prefix-length* argument is not specified, the **clear bgp ipv6 dampening** command clears route dampening information for the entire IPv6 BGP routing table.

As of Cisco IOS Release 12.3(2)T, when the *ipv6-prefix* / *prefix-length* argument is not specified, the **clear bgp ipv6 unicast dampening** command clears route dampening information for the entire IPv6 BGP routing table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast**keyword was added to Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear bgp ipv6 dampening** and the **clear bgp ipv6 unicast dampening**commands are similar to the **clear ip bgp dampening**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears route dampening information about the route to network 7000::0 and unsuppresses its suppressed routes:

```
Router# clear bgp ipv6 unicast dampening 7000::/64
```

The following example uses the **unicast** keyword and clears route dampening information about the route to network 7000::0 and unsuppresses its suppressed routes:

```
Router# clear bgp ipv6 unicast dampening 7000::/64
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp ipv6 dampened-paths	Displays IPv6 BGP dampened routes.

clear bgp ipv6 external

To clear external IPv6 Border Gateway Protocol (BGP) peers, use the **clear bgp ipv6 external**command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **external** [**soft**] [{**in** | **out**}]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
soft	(Optional) Soft reset. Does not reset the session.
in | **out**	(Optional) Triggers inbound or outbound soft reconfiguration. If the **in** or **out** option is not specified, both inbound and outbound soft resets are triggered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added to Cisco IOS Release 12.3(2)T.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast**keyword was added to Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear bgp ipv6 external**command is similar to the **clear ip bgp external** command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears the inbound session with external IPv6 BGP peers without the outbound session being reset:

```
Router# clear bgp ipv6 unicast external soft in
```

The following example uses the **unicast** keyword and clears the inbound session with external IPv6 BGP peers without the outbound session being reset:

```
Router# clear bgp ipv6 unicast external soft in
```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection by dropping all neighbor sessions.

clear bgp ipv6 flap-statistics

To clear IPv6 Border Gateway Protocol (BGP) flap statistics, use the **clear bgp ipv6 flap-statistics** command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **flap-statistics** [{*ipv6-prefix/prefix-length* | **regexp** *regexp* | **filter-list** *list*}]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) Clears flap statistics for a single entry at this IPv6 network. 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*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
regexp *regexp*	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list *list*	(Optional) Clears flap statistics for all the paths that pass the access list. The acceptable access list number range is from 1 to 199.

Command Default

No statistics are cleared. If no arguments or keywords are specified, the software clears flap statistics for all routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **multicast**keyword was added to Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clear bgp ipv6 flap-statistics**command is similar to the **clear ip bgp flap-statistics**command, except that it is IPv6-specific.

The flap statistics for a route are also cleared when an IPv6 BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears all of the flap statistics for paths that pass access list 3:

```
Router# clear bgp ipv6 unicast flap-statistics filter-list 3
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp ipv6 flap-statistics	Displays IPv6 BGP flap statistics.

clear bgp ipv6 peer-group

To clear all members of an IPv6 Border Gateway Protocol (BGP) peer group, use the **clear bgp ipv6 peer-group**command in privileged EXEC mode.

clear bgp ipv6 {**unicast** | **multicast**} **peer-group** [*name*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	BGP peer group name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added to Cisco IOS Release 12.0(26)S.
12.3(4)T	The **unicast** and **multicast**keywords were added to Cisco IOS Release 12.3(4)T.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the **clear bgp ipv6 peer-group**command without the optional *name* argument will clear all BGP peer groups.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears all IPv6 BGP peer groups:

```
Router# clear bgp ipv6 unicast peer-group
```

clear ipv6 access-list

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

clear ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

Usage Guidelines

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

The **clear ipv6 access-list**command used without the *access-list-name*argument resets the match counters for all IPv6 access lists configured on the router.

This command resets the IPv6 global ACL hardware counters.

Examples

The following example resets the match counters for the IPv6 access list named marketing:

```
Router# clear ipv6 access-list marketing
```

Related Commands

Command	Description
hardware statistics	Enables the collection of hardware statistics.

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

clear ipv6 dhcp

To clear IPv6 Dynamic Host Configuration Protocol (DHCP) information, use the **clear ipv6 dhcp**command in privileged EXEC mode:

clear ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **clear ipv6 dhcp** command deletes DHCP for IPv6 information.

Examples

The following example :

```
Router# clear ipv6 dhcp
```

clear ipv6 dhcp binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **clear ipv6 dhcp binding** command in privileged EXEC mode.

clear ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was modified. It was updated to allow for clearing all address bindings associated with a client.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)SXE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **clear ipv6 dhcp binding** command is used as a server function.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the **clear ipv6 dhcp binding** command.

If the **clear ipv6 dhcp binding** command is used with the optional *ipv6-address* argument specified, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the *ipv6-address* argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table. If the optional **vrf** *vrf-name* keyword and argument combination is used, only the bindings for the specified VRF are cleared.

Examples

The following example deletes all automatic client bindings from the DHCP for IPv6 server binding table:

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

Related Commands

Command	Description
show ipv6 dhcp binding	Displays automatic client bindings from the DHCP for IPv6 server binding table.

clear ipv6 dhcp client

To restart the Dynamic Host Configuration Protocol (DHCP) for IPv6 client on an interface, use the **clear ipv6 dhcp client** command in privileged EXEC mode.

clear ipv6 dhcp client *interface-type interface-number*

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXE.

Usage Guidelines

The **clear ipv6 dhcp client** command restarts the DHCP for IPv6 client on specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Examples

The following example restarts the DHCP for IPv6 client for Ethernet interface 1/0:

```
Router# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

clear ipv6 dhcp conflict

To clear an address conflict from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server database, use the **clear ipv6 dhcp conflict** command in privileged EXEC mode.

clear ipv6 dhcp conflict {***ipv6-address* | **vrf** *vrf-name*}

Syntax Description

*	Clears all address conflicts.
ipv6-address	Clears the host IPv6 address that contains the conflicting address.
vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

If you use the asterisk (*) character as the address parameter, DHCP clears all conflicts.

If the **vrf** *vrf-name* keyword and argument are specified, only the address conflicts that belong to the specified VRF will be cleared.

Examples

The following example shows how to clear all address conflicts from the DHCPv6 server database:

```
Router# clear ipv6 dhcp conflict *
```

Related Commands

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server when addresses are offered to the client.

clear ipv6 dhcp relay binding

To clear an IPv6 address or IPv6 prefix of a Dynamic Host Configuration Protocol (DHCP) for IPv6 relay binding, use the **clear ipv6 dhcp relay binding** command in privileged EXEC mode.

clear ipv6 dhcp relay binding{**vrf** *vrf-name*}{** ipv6-addressipv6-prefix*}

Cisco uBR10012 and Cisco uBR7200 Series Universal Broadband Devices

clear ipv6 dhcp relay binding{**vrf** *vrf-name*}{* *ipv6-prefix*}

Syntax Description

vrf *vrf-name*	Specifies a virtual routing and forwarding (VRF) configuration.
*	Clears all DHCPv6 relay bindings.
ipv6-address	DHCPv6 address.
ipv6-prefix	IPv6 prefix.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.
15.2(1)S	The command was modified to delete the binding or route for IPv6 addresses.
Cisco IOS XE Release 3.5S	The command was modified to delete the binding or route for IPv6 addresses.
12.2(33)SCF4	This command was implemented on Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **clear ipv6 dhcp relay binding** command deletes a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding. If no relay client is specified, no binding is deleted.

Examples

The following example shows how to clear the binding for a client with a specified IPv6 address:

```
Device# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

The following example shows how to clear the binding for a client with the VRF name vrf1 and a specified prefix on a Cisco uBR10012 universal broadband device:

```
Device# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/64
```

Related Commands

Command	Description
show ipv6 dhcp relay binding	Displays DHCPv6 IANA and DHCPv6 IAPD bindings on a relay agent.

clear ipv6 eigrp

To delete entries from Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing tables, use the **clear ipv6 eigrp** command in privileged EXEC mode.

clear ipv6 eigrp [*as-number*] [**neighbor** [{*ipv6-address* | *interface-type interface-number*}]]

Syntax Description

as-number	(Optional) Autonomous system number.
neighbor	(Optional) Deletes neighbor router entries.
ipv6-address	(Optional) IPv6 address of a neighboring router.
interface-type	(Optional) The interface type of the neighbor router.
interface-number	(Optional) The interface number of the neighbor router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **clear ipv6 eigrp** command without any arguments or keywords to clear all EIGRP for IPv6 routing table entries. Use the *as-number* argument to clear routing table entries on a specified process, and use the **neighbor***ipv6-address* keyword and argument, or the *interface-typeinterface-number* argument, to remove a specific neighbor from the neighbor table.

Examples

The following example removes the neighbor whose IPv6 address is 3FEE:12E1:2AC1:EA32:

```
Router# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32
```

clear ipv6 flow stats

To clear the NetFlow switching statistics, use the **clear ipv6 flow stats** command in privileged EXEC mode.

clear ipv6 flow stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show iv6 cache flow**command displays the NetFlow switching statistics. Use the **clear ipv6 flow stats**command to clear the NetFlow switching statistics.

Examples

The following example clears the NetFlow switching statistics on the router:

```
Router# clear ipv6 flow stats
```

Related Commands

Command	Description
show ipv6 flow cache	Displays the routing table cache used to fast switch IPv6 traffic.

clear ipv6 inspect

To remove a specific IPv6 session or all IPv6 inspection sessions, use the **clear ipv6 inspect**command in privileged EXEC mode.

clear ipv6 inspect {**session** *session-number* | **all**}

Syntax Description

session *session-number*	Indicates the number of the session to clear.
all	Clears all inspection sessions.

Command Default

Inspection sessions previously configured are unaffected.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example clears all inspection sessions:

```
Router# clear ipv6 inspect all
```

Related Commands

Command	Description
ipv6 inspect name	Applies a set of inspection rules to an interface.

clear ipv6 mfib counters

To reset all active Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ipv6 mfib counters** command in privileged EXEC mode.

clear ipv6 mfib [**vrf** *vrf-name*] **counters** [{*group-name*|*group-address* [{*source-addresssource-name*}]}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
source-address | *source-name*	(Optional) IPv6 address or name of the source.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

After you enable the **clear ipv6 mfib counters** command, you can determine if additional traffic is forwarded by using one of the following show commands that display traffic counters:

- **show ipv6 mfib**
- **show ipv6 mfib active**
- **show ipv6 mfib count**
- **show ipv6 mfib interface**
- **show ipv6 mfib summary**

Examples

The following example clears and resets all MFIB traffic counters:

```
Router# clear ipv6 mfib counters
```

clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the **clear ipv6 mld counters** command in privileged EXEC mode.

clear ipv6 mld [**vrf** *vrf-name*] **counters** [*interface-type*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **clear ipv6 mld counters** command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional *interface-type* argument, the **clear ipv6 mld counters**command clears the counters on all interfaces.

Examples

The following example clears the counters for Ethernet interface 1/0:

```
Router# clear ipv6 mld counters Ethernet1/0
```

Related Commands

Command	Description
show ipv6 mld interface	Displays multicast-related information about an interface.

clear ipv6 mld traffic

To reset the Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Using the **clear ipv6 mld traffic** command will reset all MLD traffic counters.

Examples

The following example resets the MLD traffic counters:

```
Router# clear ipv6 mld traffic
```

Command	Description
show ipv6 mld traffic	Displays the MLD traffic counters.

IPv6 Commands: clear ipv6 mo to ct

- ctunnel mode, on page 117

clear ipv6 mobile binding

To clear the Mobile IPv6 binding cache on a router, use the **clear ipv6 mobile binding**command in privileged EXEC mode.

clear ipv6 mobile binding [{**care-of-address** *prefix* | **home-address** *prefix* | *interface-type interface-number*}]

Syntax Description

care-of-address	(Optional) Provides information about the mobile node's current location.
prefix	(Optional) IPv6 address prefix of the care-of address or the home address.
home-address	(Optional) IPv6 address assigned to the mobile node within its home subnet prefix on its home link.
interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **clear ipv6 mobile binding** command clears the binding caches for a specified mobile node (if specified) or all mobile nodes (if no arguments or keywords are specified).

The *prefix* argument can be a prefix for the care-of address or the home address of a mobile node, so that entire networks can be cleared. Enter /**128** to clear an individual mobile node.

Use of this command with the *interface-type*and *interface-number* arguments clears all bindings on the specified interface.

Examples

In the following example, the binding caches for all mobile nodes are cleared:

```
Router# clear ipv6 mobile binding
Clear 1 bindings [confirm]
Router# show ipv6 mobile binding
Mobile IPv6 Binding Cache Entries:
Selection matched 0 bindings
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
show ipv6 mobile binding	Displays information about the binding cache.

clear ipv6 mobile home-agents

To clear the neighboring home agents list, use the **clear ipv6 mobile home-agents**command in privileged EXEC mode.

clear ipv6 mobile home-agents [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **clear ipv6 mobile home-agents** command clears the neighboring home agents list. The list is subsequently reconstructed from received router advertisements.

If you do not enter the optional *interface type* and *interface-number*arguments, the home agent lists on all interfaces are cleared.

Examples

In the following example, the neighboring home agent lists are cleared:

```
Router# clear ipv6 mobile home-agents
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
show ipv6 mobile home-agent	Displays neighboring home agents.

clear ipv6 mobile traffic

To clear statistics associated with Mobile IPv6 traffic, use the **clear ipv6 mobile traffic**command in privileged EXEC mode.

clear ipv6 mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **clear ipv6 mobile traffic** command clears the statistics about the received binding updates and transmitted binding acknowledgments on a mobile node.

Examples

In the following example, statistics about binding updates and binding acknowledgments are cleared:

```
Router# clear ipv6 mobile traffic

Router# show ipv6 mobile traffic
MIPv6 statistics:
  Rcvd: 0 total
      0 truncated, 0 format errors
      0 checksum errors
    Binding Updates received:0
      0 no HA option, 0 BU's length
      0 options' length, 0 invalid CoA
  Sent: 0 generated
    Binding Acknowledgements sent:0
      0 accepted (0 prefix discovery required)
      0 reason unspecified, 0 admin prohibited
      0 insufficient resources, 0 home reg not supported
      0 not home subnet, 0 not home agent for node
      0 DAD failed, 0 sequence number
    Binding Errors sent:0
      0 no binding, 0 unknown MH
  Home Agent Traffic:
    0 registrations, 0 deregistrations
    unknown time since last accepted HA registration
    unknown time since last failed HA registration
    unknown last failed registration code
    Traffic forwarded:
      0 tunneled, 0 reversed tunneled
    Dynamic Home Agent Address Discovery:
      0 requests received, 0 replies sent
    Mobile Prefix Discovery:
      0 solicitations received, 0 advertisements sent
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
show ipv6 mobile home-agent	Displays neighboring home agents.

clear ipv6 mtu

To clear the maximum transmission unit (MTU) cache of messages, use the **clear ipv6 mtu**command in privileged EXEC mode.

clear ipv6 mtu

Syntax Description

This command has no arguments or keywords.

Command Default

Messages are not cleared from the MTU cache.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If a router is flooded with ICMPv6 toobig messages, the router is forced to create an unlimited number of entries in the MTU cache until all available memory is consumed. Use the **clear ipv6 mtu** command to clear messages from the MTU cache.

Examples

The following example clears the MTU cache of messages:

```
Router# clear ipv6 mtu
```

Related Commands

Command	Description
ipv6 flowset	Configures flow-label marking in 1280-byte or larger packets sent by the router.

clear ipv6 multicast aaa authorization

To clear authorization parameters that restrict user access to an IPv6 multicast network, use the **clear ipv6 multicast aaa authorization**command in privileged EXEC mode.

clear ipv6 multicast aaa authorization [*interface-type interface-number*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Using the **clear ipv6 multicast aaa authorization**command without the optional *interface-type* and *interface-number* arguments will clear all authorization parameters on a network.

Examples

The following example clears all configured authorization parameters on an IPv6 network:

```
Router# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

Related Commands

Command	Description
aaa authorization multicast default	Sets parameters that restrict user access to an IPv6 multicast network.

clear ipv6 nat translation

To clear dynamic Network Address Translation--Protocol Translation (NAT-PT) translations from the dynamic state table, use the **clear ipv6 nat translation**command in privileged EXEC mode.

clear ipv6 nat translation *

Syntax Description

*	Clears all dynamic NAT-PT translations.

Command Default

Entries are deleted from the dynamic translation state table when they time out.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use this command to clear entries from the dynamic translation state table before they time out. Static translation configuration is not affected by this command.

Examples

The following example shows the NAT-PT entries before and after the dynamic translation state table is cleared. Note that all the dynamic NAT-PT mappings are cleared, but the static NAT-PT configurations remain.

```
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69
Router# clear ipv6 nat translation *
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
```

Related Commands

Command	Description
ipv6 nat	Designates that traffic originating from or destined for the interface is subject to NAT-PT.
show ipv6 nat translations	Displays active NAT-PT translations.

clear ipv6 nd destination

To clear IPv6 host-mode destination cache entries, use the **clear ipv6 nd destination** command in privileged EXEC mode.

clear ipv6 nd destination [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

The **clear ipv6 nd destination** command clears IPv6 host-mode destination cache entries. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is cleared.

Examples

The following example shows how to clear IPv6 host-mode destination cache entries:

```
Device# clear ipv6 nd destination
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

clear ipv6 nd on-link prefix

To clear on-link prefixes learned through router advertisements (RAs), use the **clear ipv6 nd on-link prefix** command in privileged EXEC mode.

clear ipv6 nd on-link prefix [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **clear ipv6 nd on-link prefix** command to clear locally reachable IPv6 addresses (e.g., on-link prefixes) learned through RAs. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is cleared.

Examples

The following examples shows how to clear on-link prefixes learned through RAs:

```
Device# clear ipv6 nd on-link prefix
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

clear ipv6 nd router

To clear neighbor discovery (ND) device entries learned through router advertisements (RAs), use the **clear ipv6 nd router** command in privileged EXEC mode.

clear ipv6 nd router [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **clear ipv6 nd router** command to clear ND device entries learned through RAs. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is cleared.

Examples

The following example shows how to clear neighbor discovery ND device entries learned through RAs:

```
Device# clear ipv6 nd router
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries and ND cache entries on non-virtual routing and forwarding (VRF) interfaces, use the **clear ipv6 neighbors** command in privileged EXEC mode.

Syntax for Releases 15.0(1)M, 12.2(33)SXH, and 12.2(33)SRC, and Later Releases
clear ipv6 neighbors [{**interface** *type number* [**ipv6** *ipv6-address*] | **statistics** | **vrf** *table-name* [{*ipv6-address* | **statistics**}]}]

Syntax for Release Cisco IOS XE Release 2.1 and Later Releases
clear ipv6 neighbors

Syntax Description

interface *type number*	(Optional) Clears the IPv6 neighbor discovery cache in the specified interface.
ipv6 *ipv6-address*	(Optional) Clears the IPv6 neighbor discovery cache that matches the specified IPv6 address on the specified interface.
statistics	(Optional) Clears the IPv6 neighbor discovery entry cache.
vrf	(Optional) Clears entries for a virtual private network (VPN) routing or forwarding instance.
table-name	(Optional) Table name or identifier. The value range is from 0x0 to 0xFFFFFFFF (0 to 65535 in decimal).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** keyword and *table-name* argument were added.

Release	Modification
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **clear ipv6 neighbor** command clears ND cache entries. If the command is issued without the **vrf** keyword, then the command clears ND cache entries on interfaces associated with the default routing table (e.g., those interfaces that do not have a **vrf forwarding** statement). If the command is issued with the **vrf** keyword, then it clears ND cache entries on interfaces associated with the specified VRF.

Examples

The following example deletes all entries, except static entries and ND cache entries on non-VRF interfaces, in the neighbor discovery cache:

```
Device# clear ipv6 neighbors
```

The following example clears all IPv6 neighbor discovery cache entries, except static entries and ND cache entries on non-VRF interfaces, on Ethernet interface 0/0:

```
Device# clear ipv6 neighbors interface Ethernet 0/0
```

The following example clears a neighbor discovery cache entry for 2001:0DB8:1::1 on Ethernet interface 0/0:

```
Device# clear ipv6 neighbors interface Ethernet0/0 ipv6 2001:0DB8:1::1
```

In the following example, interface Ethernet 0/0 is associated with the VRF named red. Interfaces Ethernet 1/0 and Ethernet 2/0 are associated with the default routing table (because they are not associated with a VRF). Therefore, the **clear ipv6 neighbor** command will clear ND cache entries on interfaces Ethernet 1/0 and Ethernet 2/0 only. In order to clear ND cache entries on interface Ethernet 0/0, the user must issue the **clear ipv6 neighbor vrf** red command.

```
interface ethernet0/0
  vrf forward red
  ipv6 address 2001:db8:1::1/64

interface ethernet1/0
   ipv6 address 2001:db8:2::1/64

interface ethernet2/0
   ipv6 address 2001:db8:3::1/64
```

Related Commands

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

clear ipv6 nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ipv6 nhrp**command in privileged EXEC mode.

clear ipv6 nhrp [{*ipv6-address* | **counters**}]

Syntax Description

ipv6-address	(Optional) The IPv6 network to delete.
counters	(Optional) Specifies NHRP counters to delete.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command does not clear any static (configured) IPv6-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

Examples

The following example shows how to clear all dynamic entries from the NHRP cache for the interface:

```
Router# clear ipv6 nhrp
```

Related Commands

Command	Description
show ipv6 nhrp	Displays the NHRP cache.

clear ipv6 ospf

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **cl ear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] {**process** | **force-spf** | **redistribution**}

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
process	Restarts the OSPF process.
force-spf	Starts the shortest path first (SPF) algorithm without first clearing the OSPF database.
redistribution	Clears OSPF route redistribution.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.

Usage Guidelines

When the **process** keyword is used with the **clear ipv6 ospf**command, the OSPF database is cleared and repopulated, and then the shortest path first (SPF) algorithm is performed. When the **force-spf**keyword is used with the **clear ipv6 ospf**command, the OSPF database is not cleared before the SPF algorithm is performed.

Use the *process-id*option to clear only one OSPFprocess. If the *process-id*optionis not specified,all OSPF processesare cleared.

Examples

The following example starts the SPF algorithm without clearing the OSPF database:

```
Router# clear ipv6 ospf force-spf
```

clear ipv6 ospf counters

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the **cl ear ipv6 ospf** command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] **counters** [**neighbor** [{*neighbor-interfaceneighbor-id*}]]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
neighbor	(Optional) Neighbor statistics per interface or neighbor ID.
neighbor-interface	(Optional) Neighbor interface.
neighbor-id	(Optional) IPv6 or IP address of the neighbor.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **neighbor***neighbor-interface* option to clear counters for all neighbors on a specified interface. If the **neighbor***neighbor-interface* option is not used, all OSPF counters are cleared.

Use the **neighbor** *neighbor-id*option to clear counters at a specified neighbor. If the **neighbor** *neighbor-id*optionis not used,all OSPF counters are cleared.

Examples

The following example provides detailed information on a neighbor router:

```
Router# show ipv6 ospf neighbor detail
 Neighbor 10.0.0.1
    In the area 1 via interface Serial19/0
    Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x194AE05
    Dead timer due in 00:00:37
    Neighbor is up for 00:00:15
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
```

```
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following example clears all neighbors on the specified interface:

```
Router# clear ipv6 ospf counters neighbor s19/0
```

The following example now shows that there have been 0 state changes since the **clear ipv6 ospf counters neighbor s19/0** command was used:

```
Router# show ipv6 ospf neighbor detail
 Neighbor 10.0.0.1
    In the area 1 via interface Serial19/0
    Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
    Neighbor priority is 1, State is FULL, 0 state changes
    Options is 0x194AE05
    Dead timer due in 00:00:39
    Neighbor is up for 00:00:43
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
show ipv6 ospf neighbor	Displays OSPF neighbor information on a per-interface basis.

clear ipv6 ospf events

To clear the Open Shortest Path First (OSPF) for IPv6 event log content based on the OSPF routing process ID, use the **cl ear ipv6 ospf events**command in privileged EXEC mode.

clear ipv6 ospf [*process-id*] **events**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the optional *process-id* argument to clear the IPv6 event log content of a specified OSPF routing process. If the *process-id* argument is not used, all event log content is cleared.

Examples

The following example enables the clearing of OSPF for IPv6 event log content for routing process 1:

```
Router# clear ipv6 ospf 1 events
```

clear ipv6 pim counters

To reset the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim counters** command in privileged EXEC mode.

clear ipv6 pim counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the **clear ipv6 pim counters**command will reset all PIM traffic counters.

Examples

The following example resets the PIM traffic counters:

```
Router# clear ipv6 pim counters
```

Related Commands

Command	Description
show ipv6 pim traffic	Displays the PIM traffic counters.

clear ipv6 pim limit

To clear Protocol Independent Multicast (PIM) statistics, use the **clear ipv6 pim limit** command in privileged EXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which statistics will be cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **clear ipv6 pim limit** command clears IPv6 PIM interface statistics. If the optional *interface* argument is enabled, only statistics for the specified interface are cleared.

Examples

The following example clears PIM interface limit statistics:

```
Router# clear ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

clear ipv6 pim reset

To delete all entries from the topology table and reset the Multicast Routing Information Base (MRIB) connection, use the **clear ipv6 pim reset**command inprivilegedEXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **reset**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Using the **clear ipv6 pim reset** command breaks the PIM-MRIB connection, clears the topology table, and then reestablishes the PIM-MRIB connection. This procedure forces MRIB resynchronization.

Caution Use the **clear ipv6 pim reset** command with caution, as it clears all PIM protocol information from the PIM topology table. Use of the **clear ipv6 pim reset** command should be reserved for situations where PIM and MRIB communication are malfunctioning.

Examples

The following example deletes all entries from the topology table and resets the MRIB connection:

```
Router# clear ipv6 pim reset
```

clear ipv6 pim topology

To clear the Protocol Independent Multicast (PIM) topology table, use the **clear ipv6 pim topology** command inprivilegedEXEC mode.

clear ipv6 pim [**vrf** *vrf-name*] **topology** [{*group-namegroup-address*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.

Command Default

When the command is used with no arguments, all group entries located in the PIM topology table are cleared of PIM protocol information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

This command clears PIM protocol informationfrom all group entries located in the PIM topology table. Information obtained from the MRIB table is retained. If a multicast group is specified, only those group entries are cleared.

Examples

The following example clears all group entries located in the PIM topology table:

```
Router# clear ipv6 pim topology
```

clear ipv6 pim traffic

To clear the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim traffic**command inprivilegedEXEC mode.

clear **ipv6** **pim** [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

When the command is used with no arguments, all traffic counters are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command clears PIM traffic counters. If the **vrf** *vrf-name* keyword and argument are used, only those counters are cleared.

Examples

The following example clears all PIM traffic counter:

```
Router# clear ipv6 pim traffic
```

clear ipv6 prefix-list

To reset the hit count of the IPv6 prefix list entries, use the **clear ipv6 prefix-list**command in privileged EXEC mode.

clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-prefix/prefix-length*]

Syntax Description

prefix-list-name	(Optional) The name of the prefix list from which the hit count is to be cleared.
ipv6-prefix	(Optional) The IPv6 network from which the hit count is to be cleared. 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*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

The hit count is automatically cleared for all IPv6 prefix lists.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

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

The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35.

```
Router# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

clear ipv6 rip

To delete routes from the IPv6 Routing Information Protocol (RIP) routing table, use the **clear ipv6 rip** command in privileged EXEC mode.

Cisco IOS Release XE 3.9S, Cisco IOS Release 15.3(2)S, and Later Releases

clear ipv6 rip [*name*] [**vrf** *vrf-name*]

Releases Prior to Cisco IOS XE Release 3.9S and Cisco IOS Release 15.3(2)S
clear ipv6 rip [*name*]

Syntax Description

name	(Optional) Name of an IPv6 RIP process.
vrf *vrf-name*	(Optional) Clears information about the specified Virtual Routing and Forwarding (VRF) instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S. The **vrf** *vrf-name* keyword/argument pair was added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

When the *name* argument is specified, only routes for the specified IPv6 RIP process are deleted from the IPv6 RIP routing table. If no *name* argument is specified, all IPv6 RIP routes are deleted.

Use the **show ipv6 rip** command to display IPv6 RIP routes.

Use the **clear ipv6 rip** *name* **vrf** *vrf-name* command to delete the specified VRF instances for the specified IPv6 RIP process.

Examples

The following example deletes all the IPv6 routes for the RIP process called one:

```
Device# clear ipv6 rip one
```

The following example deletes the IPv6 VRF instance, called vrf1 for the RIP process, called one:

```
Device# clear ipv6 rip one vrf vrf1

*Mar 15 12:36:17.022: RIPng: Deleting 2001:DB8::/32
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete all next-hops for 2001:DB8::1
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete 2001:DB8::1 from table
*Mar 15 12:36:17.022: [IPv6 RIB Event Handler]IPv6RT[<red>]: Event: 2001:DB8::1, Del, owner
 rip, previous None
```

Related Commands

Command	Description
debug ipv6 rip	Displays the current contents of the IPv6 RIP routing table.
ipv6 rip vrf-mode enable	Enables VRF-aware support for IPv6 RIP.
show ipv6 rip	Displays the current content of the IPv6 RIP routing table.

clear ipv6 route

To delete routes from the IPv6 routing table, use the **clear ipv6 route**command in privileged EXEC mode.

{**clear ipv6 route** {*ipv6-addressipv6-prefix/prefix-length*} | *****}

Syntax Description

ipv6-address	The address of the IPv6 network to delete from the table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	The IPv6 network number to delete from the table. 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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
*****	Clears all IPv6 routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **clear ipv6 route**command is similar to the **clear ip route**command, except that it is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix*/ *prefix-length* argument is specified, only that route is deleted from the IPv6 routing table. When the ***** keyword is specified, all routes are deleted from the routing table (the per-destination maximum transmission unit [MTU] cache is also cleared).

Examples

The following example deletes the IPv6 network 2001:0DB8::/35:

```
Router# clear ipv6 route 2001:0DB8::/35
```

Related Commands

Command	Description
ipv6 route	Establishes static IPv6 routes.
show ipv6 route	Displays the current contents of the IPv6 routing table.

clear ipv6 snooping counters

To remove counter entries, use the **clear ipv6 snooping counters**command in privileged EXEC mode.

clear ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Clears the counter of entries that match the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **clear ipv6 snooping counters**command removes counters from all the configured interfaces. You can use the optional **interface** *type number* keyword and argument to remove counters from the specified interface.

Examples

The following example shows how to remove entries from the counter:

```
Router# clear
 ipv6 snooping counters
```

clear ipv6 spd

To clear the most recent Selective Packet Discard (SPD) state transition, use the **clear ipv6 spd**command in privileged EXEC mode.

clear ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **clear ipv6 spd** command removes the most recent SPD state transition and any trend historical data.

Examples

The following example shows how to clear the most recent SPD state transition:

```
Router# clear ipv6 spd
```

clear ipv6 traffic

To reset IPv6 traffic counters, use the **clear ipv6 traffic**command in privileged EXEC mode.

clear ipv6 traffic [*interface-type interface-number*]

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S and output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)XN	The optional *interface-type* and *interface-number* arguments were added.

Usage Guidelines

Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples

The following example resets the IPv6 traffic counters. The output from the **show ipv6 traffic** command shows that the counters are reset:

```
Router# clear ipv6 traffic
Router# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 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 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
```

```
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output
TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

clear ipv6 wccp

To remove IPv6 Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the **clear ipv6 wccp** command in privileged EXEC mode.

clear ipv6 wccp [**vrf***vrf-name*] [*service-number*] [**web-cache**] [**default**]

Syntax Description

vrf *vrf-name*	(Optional) Directs the router to remove statistics for a specific virtual routing and forwarding (VRF) instance.
service-number	(Optional) Number of the cache service to be removed. The number can be from 0 to 254.
web-cache	(Optional) Directs the router to remove statistics for the web cache service.
default	(Optional) Directs the router to remove statistics for the default routing table.

Command Default

WCCP statistics are not removed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Use the **show ipv6 wccp** and **show ipv6 wccp detail** commands to display WCCP statistics. If Cisco Cache Engines are used in your service group, the reverse proxy service is indicated by a value of 99.

Use the **clear ipv6 wccp** command to clear the WCCP counters for all WCCP services in all VRFs.

Examples

The following example shows how to clear all statistics associated with the web cache service:

```
Router# clear ipv6 wccp web-cache
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.
show ipv6 wccp	Displays global statistics related to the WCCP.

clear mls cef ipv6 accounting per-prefix

To clear information about the IPv6 per-prefix accounting statistics, use the **clear mls cef ipv6 accounting per-prefix**command in privileged EXEC mode.

clear mls cef ipv6 accounting per-prefix {**all** | *ipv6-address/mask* [*instance*]}

Syntax Description

all	Clears all per-prefix accounting statistics information.
ipv6-address / *mask*	Entry IPv6 address and mask. The format used is X:X:X:X::X/ *mask,*where the valid values for *mask* are from 0 to 128.
instance	(Optional) VPN routing and forwarding instance name.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When entering the *ipv6-address* / *mask* arguments, use this format, X:X:X:X::X/*mask,*where the valid values for *mask* are from 0 to 128.

Examples

This example shows how to clear all information about the per-prefix accounting statistics:

```
Router#
clear mls cef ipv6 accounting per-prefix all
```

clear ospfv3 counters

To clear Open Shortest Path First version 3 (OSPFv3) counters, use the **clear ospfv3 counters** command in privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}] **counters** [**neighbor** [{*neighbor-interfaceneighbor-id*}]]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.
neighbor	(Optional) Neighbor statistics per interface or neighbor ID.
neighbor-interface	(Optional) Specified neighbor interface.
neighbor-id	(Optional) IPv6 or IPv4 address of the neighbor.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **neighbor***neighbor-interface* option to clear counters for all neighbors on a specified interface. If the **neighbor***neighbor-interface* option is not used, all OSPFv3 counters are cleared.

Examples

The following example clears all neighbors on the serial 19/0 interface:

```
Router# clear ospfv3 counters neighbor s19/0
```

clear ospfv3 force-spf

To run shortest path first (SPF) calculations for an Open Shortest Path First version 3 (OSPFv3) process, use the **clear ospfv3 force-spf** command in privileged EXEC mode.

clear **ospfv3** [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}] **force-spf**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **clear ospv3 force-spf**command to run SPF calculations for either an IPv6 or an IPv4 OSPFv3 instance. If the optional *process-ID* argument is not used, SPF runs on all instances on the interface. <<OK?>>

Examples

The following example enables SPF calculations for process 1:

```
Router# clear ospfv3 1 force-spf
```

clear ospfv3 process

To reset an Open Shortest Path First version 3 (OSPFv3) process, use the **clear ospfv3 process**command in privileged EXEC mode.

clear ospfv3 process [*process-id*] [*address family*] [**vrf** {*vrf-name* | *****}]
nsr [**synchronization** | **statistics**]

Syntax Description

process *process-id*	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.
synchronization	(Optional) Causes OSPFv3 on the standby Route Processor (RP) to reset and resynchronize with the active RP.
statistics	(Optional) Resets statistical counters maintained for NSR.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **clear ospv3 process**command to reset either an IPv6 or IPv4 OSPFv3 process. If the optional *process-ID* argument is not used, all OSPFv3 processes are reset.

Examples

The following example resets the OSPFv3 process 2:

```
Router# clear ospfv3 2 process
```

clear ospfv3 redistribution

To clear Open Shortest Path First version 3 (OSPFv3) route redistribution, use the **clear ospfv3 redistribution**command in privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}] **redistribution**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **clear ospv3 process**command to clear either IPv6 or IPv4 OSPFv3 redistribution. If the optional *process-ID* argument is not used, all processes on the interface are cleared. <<OK?>>

Examples

The following example clears OSPFv3 redistribution on all OSPFv3 processes:

```
Router# clear ospfv3 redistribution
```

clear ospfv3 traffic neighbor

To reset counters and clear Open Shortest Path First version 3 (OSPFv3) traffic and neighbor statistics, use the **clear ospfv3 traffic neighbor** command privileged EXEC mode.

clear ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}] **traffic** [*interface*] **neighbor**[*interface* [*neighbor-id*]]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.
interface	(Optional) Specified interface from which to clear traffic statistics.
interface [*neighbor-id*]	Specifies interface and neighbor traffic statistics from one interface and all neighbors on that interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **clear ospv3 traffic neighbor** command to reset neighbor traffic statistics for an IPv6 or IPv4 OSPFv3 process. If the optional *process-ID* argument is not used, all traffic statistics are cleared.

Examples

The following example resets the counters and clears the OSPFv3 traffics statistics:

```
Router# clear ospfv3 traffic
```

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **compatible rfc1583**command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583
no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Command Default

Compatible with RFC 1583.

Command Modes

Router configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is backward compatible with Cisco IOS Release 12.0.

To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the no compatible rfc1583 command to enable the calculation method used per RFC 2328.

Examples

The following example specifies that the router process is compatible with RFC 1583:

```
router ospf 1
 compatible rfc1583
 !
```

ctunnel mode

To transport IPv4 and IPv6 packets over Connectionless Network Service (CLNS) tunnel (CTunnel), use the **ctunnelmode** command in interface configuration mode. To return the ctunnel to the default **cisco** mode, use the **no** form of this command.

ctunnel mode [{**gre** | **cisco**}]
no ctunnel mode

Syntax Description

gre	(Optional) Sets the ctunnel mode to Generic Routing Encapsulation (GRE) for transporting IPv6 packets over the CLNS network.
cisco	(Optional) Returns the ctunnel mode to the default cisco.

Command Default

Cisco encapsulation tunnel mode is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

GRE tunneling of IPv4 and IPv6 packets through CLNS-only networks enables Cisco ctunnels to interoperate with networking equipment from other vendors. This feature provides compliance with RFC 3147, Generic Routing Encapsulation over CLNS Networks, which should allow interoperation between Cisco equipment and that of other vendors. in which the same standard is implemented.

RFC 3147 specifies the use of GRE when tunneling packets. The implementation of this feature does not include support for GRE header fields such as those used to specify checksums, keys, or sequencing. Any packets received which specify the use of these features will be dropped.

The default ctunnel mode continues to use the standard Cisco encapsulation. Both ends of the tunnel must be configured with the same mode for it to work. If you want to tunnel ipv6 packets you must use the new gre mode.

Examples

The following example configures a CTunnel from one router to another and shows the CTunnel destination set to 49.0001.1111.1111.1111.00. The ctunnel mode is set to gre to transport IPv6 packets.

```
interface ctunnel 301
 ipv6 address 2001:0DB8:1111:2222::2/64
```

```
ctunnel destination 49.0001.1111.1111.1111.00
ctunnel mode gre
```

Related Commands

Command	Description
clns routing	Enables routing of CLNS packets.
ctunnel destination	Specifies the destination for the CTunnel.
debug ctunnel	Displays debug messages for the IP over a CLNS Tunnel feature.
interface ctunnel	Creates a virtual interface to transport IP over a CLNS tunnel.
ip address	Sets a primary or secondary IP address for an interface.

IPv6 Commands: d to im

data-glean

To enable IPv6 first-hop security binding table recovery using source (or 'data') address gleaning, or to generate syslog messages about unrecognized binding table entries following a recovery, use the **destination-glean** command in IPv6 snooping configuration mode. To disable binding table recovery, use the **no** form of this command.

data-glean {**recovery** | **log-only**} [{**dhcp** | **ndp**}]
no data-glean

Syntax Description

recovery	Enables binding table recovery using destination address gleaning.
log-only	Generates a syslog message about unrecognized binding table entries following a recovery.
dhcp	Specifies that destination addresses should be recovered from Dynamic Host Configuration Protocol (DHCP).
ndp	Specifies that destination addresses should be recovered from Neighbor Discovery Protocol (NDP).

Command Default

IPv6 first-hop security binding table recovery using destination address gleaning is not enabled.

Command Modes

IPv6 snooping configuration mode (config-ipv6-snooping)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

When you configure IPv6 source guard using the **ipv6 source-guard policy** command, you can then also configure IPv6 first-hop security binding table recovery.

The **ipv6 snooping policy** command allows you to configure a snooping policy. You can configure first-hop security binding table recovery as part of this policy. The snooping policy can then be attached to a port, VLAN, or interface (depending on the device being used) using the **ipv6 snooping attach-policy** command.

If you use the **data-glean** command with the **log-only** keyword, only a syslog message will be generated and no recovery will be attempted.

Examples

The following example shows that destination addresses should be recovered from DHCP:

```
Device(config-ipv6-snooping)# data-glean recovery dhcp
```

The following example shows that a syslog message will be generated for all missed destination addresses following a binding table recovery:

```
Device(config-ipv6-snooping)# data-glean log-only
```

Related Commands

Command	Description
ipv6 source-guard policy	Configures an IPv6 source guard policy.
ipv6 snooping policy	Enters IPv6 snooping configuration mode.

default (IPv6 OSPF)

To return a parameter to its default value, use the **default**command in router configuration mode.

default [{**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**}]

Syntax Description

area	(Optional) Open Shortest Path First (OSPF) for IPv6 area parameters.
auto-cost	(Optional) OSPF interface cost according to bandwidth.
default-information	(Optional) Distributes default information.
default-metric	(Optional) Metric for a redistributed route.
discard-route	(Optional) Enables or disables discard-route installation.
distance	(Optional) Administrative distance.
distribute-list	(Optional) Filter networks in routing updates.
ignore	(Optional) Ignores a specific event.
log-adjacency-changes	(Optional) Log changes in the adjacency state.
maximum-paths	(Optional) Forwards packets over multiple paths.
passive-interface	(Optional) Suppresses routing updates on an interface.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
router-id	(Optional) Router ID for the specified routing process.
summary-prefix	(Optional) OSPF summary prefix.
timers	(Optional) OSPF timers.

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The command is removed if it is disabled by default.

Examples

In the following example, OSPF for IPv6 area parameters are reset to the default values:

```
default timers spf
```

default (OSPFv3)

To return an Open Shortest Path First version 3 (OSPFv3) parameter to its default value, use the **default**command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode.

default area *area-ID* [{**range** *ipv6-prefix* | **virtual-link** *router-id*}] [{**default-information originate** [{**always** | **metric** | **metric-type** | **route-map**}] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*}]

Syntax Description

area	OSPFv3 area parameters.
area-ID	Area ID associated with the OSPFv3 interface.
range	Summarizes routes that match the address or address mask on border routers only.
ipv6-prefix	An IPv6 address.
virtual-link	Defines a virtual link and its parameters.s
router-id	Router ID associated with the virtual-link neighbor.
default-information originate	(Optional) Distribution of default route information.
always	(Optional) Always provides the default route information.
metric	(Optional) Provides the OSPFv3 default metric.
metric-type	(Optional) Provides the OSPFv3 metric type for default routes.
route-map	(Optional) Provides the route-map reference.
distance	(Optional) Provides the administrative distance.
distribute-list	(Optional) Filter networks in routing updates.
prefix-list *prefix-list-name*	Filters connections based on an IPv6 prefix list.
in	Filters incoming routing updates.
out	Filters outgoing routing updates.
interface	(Optional) Filters incoming or outgoing routing updates on a specified interface.
maximum-paths	(Optional) Forwards packets over multiple paths.
paths	Maximum number of paths. The range is from 1 through 32.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
protocol	The routing protocol from which IPv6 prefixes are redistributed.

summary-prefix	(Optional) OSPFv3 summary prefix.

Command Default

This command is disabled by default.

Command Modes

OSPFv3 router configuration mode (config-router)
IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **default**command in OSPFv3 router configuration mode to reset OSPFv3 parameters for an IPv4 OSPFv3 process.

Use the **default**command in IPv6 or IPv4 address family configuration mode to reset OSPFv3 parameters for an IPv6 or an IPv4 process.

Examples

In the following example, OSPFv3 parameters are reset to the default value for area 1 in IPv6 address family configuration mode:

```
Router(config-router)# address-family ipv6 unicast

Router(config-router-af)# default area 1
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

default-information originate (IPv6 IS-IS)

To inject an IPv6 default route into an Intermediate System-to-Intermediate System (IS-IS) IPv6 routing domain, use the **default-information originate** command in address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]
no default-information originate [**route-map** *map-name*]

Syntax Description

route-map *map-name*	(Optional) Route map should be used to advertise the default route conditionally. The *map-name* argument identifies a configured route map.

Command Default

This feature is disabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **default-information originate**(IPv6 IS-IS) command is similar to the **default-information originate**(IS-IS) command, except that it is IPv6-specific.

If a router configured with this command has an IPv6 route to ::/0 in the routing table, IS-IS will originate an advertisement for ::/0 in its link-state packets (LSPs).

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is for the router to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.
- Advertise ::/0 conditionally.

With a **match ipv6 address** *standard-access-list* command, you can specify one or more IPv6 routes that must exist before the router will advertise ::/0.

Examples

The following example shows the IPv6 default route (::/0) being advertised with all other routes in router updates:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# default-information originate
```

Related Commands

Command	Description
address-family ipv6 (IS-IS)	Specifies the IPv6 address family and places the router in address family configuration mode.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show isis database	Displays the IS-IS link-state database.

default-information originate (IPv6 OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) for IPv6 routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]
no default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric *metric-value*	Metric used for generating the default route. If you omit a value and do not specify a value using the **default-metric** router configuration command, the default metric value is 10. The default metric value range is from 0 to 16777214.
metric-type *type-value*	(Optional) External link type associated with the default route advertised into the OSPF for IPv6 routing domain. It can be one of the following values: **1**--Type 1 external route **2**--Type 2 external route The default is type 2 external route.
route-map *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Whenever you use the **redistribute** or the **default-information** router configuration command to redistribute routes into an OSPF for IPv6 routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF for IPv6 routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPF for IPv6 process, the default network must reside in the routing table, and you must satisfy the **route-map** *map-name* keyword and argument. Use the **default-information originate always route-map** *map-name* form of the command when you do not want the dependency on the default network in the routing table.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPF for IPv6 routing domain, an external metric type of type 2, and the default route to be always advertised:

```
default-information originate always metric 100 metric-type 2
```

Related Commands

Command	Description
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

default-information originate (OSPFv3)

To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) for a routing domain, use the **default-information originate** command in IPv6 or IPv4 address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [{**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*}]
no default-information originate [{**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*}]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric *metric-value*	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the **default-metric** router configuration command, the default metric value is 10. The default metric value range is from 0 to 16777214.
metric-type *type-value*	(Optional) External link type associated with the default route advertised into the OSPF for IPv6 routing domain. It can be one of the following values: **1** --Type 1 external route **2** --Type 2 external route The default is type 2 external route.
route-map *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Command Default

This command is disabled by default.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Whenever you use the **redistribute** or the **default-information** command to redistribute routes into an OSPFv3 routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF for IPv6 routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPFv3 process, the default network must reside in the routing table, and you must satisfy the **route-map***map-name* keyword and argument. Use the **default-information originate always route-map***map-name* form of the command when you do not want the dependency on the default network in the routing table.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPFv3 routing domain, an external metric type of type 2, and the default route to be always advertised:

```
Router(config-router-af)# default-information originate always metric 100 metric-type 2
```

default-metric (OSPFv3)

To set default metric values for IPv4 and IPv6 routes redistributed into the Open Shortest Path First version 3 (OSPF) routing protocol, use the **default-metric** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To return to the default state, use the **no** form of this command.

default-metric *metric-value*
no default-metric *metric-value*

Syntax Description

metric-value	Default metric value appropriate for the specified routing protocol. The range is from 1 to 4294967295.

Command Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Modes

OSPFv3 router configuration mode (config-router)

IPv6 address family configuration (config-router-af)

IPv4 address family configuration (config-router-af)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

You can gain finer control over the metrics of redistributed routes by using the options for the **redistribute** command.

Examples

The following example shows how to enter IPv6 AF and configure OSPFv3 routing protocol redistributing routes from the OSPFv3 process named process1. All the redistributed routes are advertised with a metric of 10.

```
router ospfv3 100
 address-family ipv6 unicast
 default-metric 10
 redistribute ospfv3 process1
```

The following example shows an OSPFv3 routing protocol redistributing routes from the OSPFv3 process named process1. All the redistributed routes are advertised with a metric of 10.

```
ipv6 router ospf 100
 default-metric 10
 redistribute ospfv3 process1
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes IPv6 routes from one routing domain into another routing domain.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

deny (IPv6)

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

deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
no deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

Internet Control Message Protocol
deny icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [{*icmp-type* [*icmp-code*]*icmp-message*}] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol
deny tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**neq** {*portprotocol*}] [**psh**] [**range** {*portprotocol*}] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol
deny udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**neq** {*portprotocol*}] [**range** {*portprotocol*}] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, **udp**, or **hbh**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.

host *source-ipv6-address*	The source IPv6 host address about which to set deny conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix*/*prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6*/*prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/*prefix-length*	The destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set deny conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with any protocol.
dest-option-type	(Optional) Matches IPv6 packets against the hop-by-hop option extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
hbh	(Optional) Specifies a hop-by-hop options header.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(Optional) Extension header type. Allows matching of any IPv6 packet including a mobility header, regardless of the value of the mobility-header-type field within that header.
mobility-type	(Optional) Mobility header type. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Name of a mobility header type. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error

routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Allows routing headers with a value in the type field to be matched independently. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
undetermined-transport	(Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration (config-ipv6-acl)#

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.2(3)T	This command was modified. Support was added for the **hbh** keyword.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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

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

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

By 1default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

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

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

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

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

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

The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header

- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on Ethernet interface 0. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of Ethernet interface 0. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of Ethernet interface 0. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of Ethernet interface 0. The second permit entry in the list permits all other traffic to exit out of Ethernet interface 0. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any
```

```
interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

The following example shows how to allow TCP or UDP parsing although an IPsec AH is present:

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

deny global-autoconf

To deny data traffic from autoconfigured global addresses, use the **deny global-autoconf** command in source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode. To disable this function, use the **no** form of this command.

deny global-autoconf
no deny global-autoconf

Syntax Description

This command has no arguments or keywords.

Command Default

Data traffic is not denied.

Command Modes

Source-guard policy configuration mode (config-source-guard)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **deny global-autoconf** command to deny data traffic from auto-configured global addresses. This function is useful when all global addresses on a link are assigned by DHCP and the administrator wants to block hosts with self-configured addresses to send traffic. Use of this command also reduces the number of ternary content addressable memory (TCAM) entries that are used.

Examples

```
Device(config)# ipv6 source-guard policy
Device(config-source-guard)# deny global-autoconf
```

Related Commands

Command	Description
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

destination-glean

To enable IPv6 first-hop security binding table recovery using destination address gleaning, or to generate syslog messages about unrecognized binding table entries following a recovery, use the **destination-glean** command in IPv6 snooping configuration mode. To disable binding table recovery, use the **no** form of this command.

destination-glean {**recovery** | **log-only**} [{**dhcp**}]
no destination-glean

Syntax Description

recovery	Enables binding table recovery using destination address gleaning.
log-only	Generates a syslog message about unrecognized binding table entries following a recovery.
dhcp	Specifies that destination addresses should be recovered from Dynamic Host Configuration Protocol (DHCP).

Command Default

IPv6 first-hop security binding table recovery using destination address gleaning is not enabled.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When you configure IPv6 destination guard using the **ipv6 destination-guard policy** command, you can then also configure IPv6 first-hop security binding table recovery.

The **ipv6 snooping policy** command allows you to configure a snooping policy. You can configure first-hop security binding table recovery as part of this policy. The snooping policy can then be attached to a port, VLAN, or interface (depending on the device being used) using the **ipv6 snooping attach-policy** command.

If you use the **destination-glean** command with the **log-only** keyword, only a syslog message will be generated and no recovery will be attempted.

Examples

The following example shows that destination addresses should be recovered from DHCP:

```
Device(config-ipv6-snooping)# destination-glean recovery dhcp
```

The following example shows that a syslog message will be generated for all missed destination addresses following a binding table recovery:

```
Device(config-ipv6-snooping)# destination-glean log-only
```

Related Commands

Command	Description
ipv6 destination-guard policy	Configures an IPv6 destination guard policy.
ipv6 snooping policy	Enters IPv6 snooping configuration mode.

device-role

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode or router advertisement (RA) guard policy configuration mode.

device-role {**host** | **monitor** | **router**}

Syntax Description

host	Sets the role of the device to host.
monitor	Sets the role of the device to monitor.
router	Sets the role of the device to router.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE. The **monitor** and **router** keywords were deprecated only from the ND inspection policy configuration (config-nd-inspection) command mode; they continue to be available in the RA guard policy configuration (config-ra-guard) mode.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The **monitor** and **router** keywords were deprecated only from the ND inspection policy configuration (config-nd-inspection) command mode; they continue to be available in the RA guard policy configuration (config-ra-guard) mode.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the **monitor** keyword does not allow inbound RA or redirect messages. When the **monitor** keyword is used, devices that need these messages will receive them.

Note With the introduction of Cisco IOS Release 15.2(4)S1, the trusted port has precedence over the device role for accepting RAs over a port to the router. Prior to this release, the device role router had precedence over the trusted port. The device role of the router still needs to be configured in order for the RS to be sent over the port.

Examples

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host
```

The following example defines an RA guard policy name as raguard1, places the device in RA guard policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

discard-route (IPv6)

To reinstall either an external or internal discard route that was previously removed, use the **discard-route** command in router configuration mode. To remove either an external or internal discard route, use the **no** form of this command.

discard-route [{**external** | **internal**}]
no discard-route [{**external** | **internal**}]

Syntax Description

external	(Optional) Reinstalls the discard route entry for redistributed summarized routes on an Autonomous System Boundary Router (ASBR).
internal	(Optional) Reinstalls the discard-route entry for summarized internal routes on the Area Border Router (ABR).

Command Default

External and internal discard route entries are installed.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

External and internal discard route entries are installed in routing tables by default. During route summarization, routing loops may occur when data is sent to a nonexisting network that appears to be a part of the summary, and the router performing the summarization has a less specific route (pointing back to the sending router) for this network in its routing table. To prevent the routing loop, a discard route entry is installed in the routing table of the ABR or ASBR.

If for any reason you do not want to use the external or internal discard route, remove the discard route by entering the **no discard-route** command with either the **external** or **internal** keyword.

Examples

The following display shows the discard route functionality installed by default. When external or internal routes are summarized, a summary route to Null0 will appear in the router output from the **show ipv6 route** command. See the router output lines that appear in bold font:

```
Router# show ipv6 route
IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
C   2001:0:11::/64 [0/0]
     via ::, Ethernet0/0
L   2001:0:11:0:A8BB:CCFF:FE00:6600/128 [0/0]
```

```
     via ::, Ethernet0/0
C   2001:1:1::/64 [0/0]
     via ::, Ethernet1/0
L   2001:1:1:0:A8BB:CCFF:FE00:6601/128 [0/0]
     via ::, Ethernet1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
Router# show ipv6 route ospf
IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
```

When the **no discard-route** command with the **internal** keyword is entered, notice the following route change, indicated by the router output lines that appear in bold font:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipv6 router ospf 1
Router(config-router)# no discard-route internal
Router(config-router)# end
Router# show ipv6 route ospf
IPv6 Routing Table - 6 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

Next, the **no discard-route** command with the **external** keyword is entered to remove the external discard route entry:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config-router)# no discard-route external
Router(config-router)# end
```

The following router output from the **show running-config** command confirms that both the external and internal discard routes have been removed from the routing table. See the router output lines that appear in bold font:

```
Router# show running-config
Building configuration...
Current configuration :2490 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
```

```
logging snmp-authfail
logging buffered 20480 debugging
logging console warnings
!
clock timezone PST -8
clock summer-time PDT recurring
no aaa new-model
ip subnet-zero
no ip domain lookup
!
!
ip audit po max-events 100
ipv6 unicast-routing
no ftp-server write-enable
!
.
.
.
interface Ethernet0/0
 no ip address
 ipv6 address 2001:0:11::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 0
 no cdp enable
!
interface Ethernet1/0
 no ip address
 ipv6 address 2001:1:1::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
 no cdp enable
 .
 .
 .
ipv6 router ospf 1
 router-id 2.0.0.1
 log-adjacency-changes
 no discard-route external
 no discard-route internal
 area 0 range 2001::/32
 redistribute rip 1
!
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.
show running config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

distance (IPv6)

To configure an administrative distance for Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), or Open Shortest Path First (OSPF) IPv6 routes inserted into the IPv6 routing table, use the **distance**command in address family configuration or router configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*
no distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

Syntax Description

ospf	(Optional) Administrative distance for OSPF for IPv6 routes.
external	External type 5 and type 7 routes for OSPF for IPv6 routes.
inter-area	Inter-area routes for OSPF for IPv6 routes.
intra-area	Intra-area routes for OSPF for IPv6 routes.
distance	The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)

Command Default

IS-IS: 115 RIP: 120 OSPF for IPv6: 110

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was implemented on the Cisco 12000 series Internet routers, and support for IS-IS was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	OSPF for IPv6 information was added. The **external**, **inter-area**, and **intra-area** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

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

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 190 for the IPv6 IS-IS routing process named area01:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# distance 190
```

The following example configures an administrative distance of 200 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# distance 200
```

The following example configures an administrative distance of 200 for external type 5 and type 7 routes for OSPF for IPv6:

```
Router(config)# ipv6 router ospf
Router(config-router)# distance ospf external 200
```

distance (IPv6 EIGRP)

To allow the use of two administrative distances--internal and external--that could be a better route to a node, use the **distance**command in router configuration mode. To reset these values to their defaults, use the **no** form of this command.

distance *internal-distance* *external-distance*
no **distance**

Syntax Description

internal-distance	Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.
external-distance	Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.

Command Default

internal-distance : 90*external-distance*: 170

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use the **distance**command if another protocol is known to be able to provide a better route to a node than was actually learned via external EIGRP for IPv6, or if some internal routes should be preferred by EIGRP for IPv6.

The table below lists the default administrative distances.

Table 3: Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5

Route Source	Default Distance
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal BGP	200
Unknown	255

Examples

The following example sets the internal distance to 95 and the external distance to 165:

```
distance 95 165
```

distance (IPv6 Mobile)

To define an administrative distance for network mobility (NEMO) routes, use the **distance** command in router configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance [*mobile-distance*]
no distance

Syntax Description

mobile-distance	(Optional) Defines the mobile route, which is the default route for IPv6 over the roaming interface. The mobile default distance is 3.

Command Default

If no distances are configured, the default distances are automatically used.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The Mobile IPv6 NEMO router maintains the following type of route:

- Mobile route--Default route for IPv6 over the roaming interface

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Examples

The following example defines the administrative distance for the mobile route as 10:

```
Router(config-router)# distance 10
```

Related Commands

Command	Description
ipv6 router nemo	Enables the NEMO routing process on the home agent and places the router in router configuration mode.

distance (OSPFv3)

To configure an administrative distance for Open Shortest Path First version 3 (OSPFv3) routes inserted into the routing table, use the **distance**command in IPv6 or IPv4 address family configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance *distance*
no distance *distance*

Syntax Description

distance	The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)

Command Default

Administrative distance is 110.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 200 for OSPFv3 in an IPv6 address family:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# distance 200
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

distance bgp (IPv6)

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family configuration mode. To return to the default values, use the **no** form of this command

distance bgp *external-distance internal-distance local-distance*
no distance bgp

Syntax Description

external-distance	Administrative distance for Border Gateway Protocol (BGP) external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.
internal-distance	Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
local-distance	Administrative distance for BGP local routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

Command Default

external-distance : 20*internal-distance*: 200*local-distance*: 200

Command Modes

Address family configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **distance bgp** (IPv6) command is similar to the **distance bgp**command, except that it is IPv6-specific. Settings configured by the **distance bgp** (IPv6) command will override the default IPv6 distance settings. IPv6 BGP is not influenced by the distance settings configured in IPv4 BGP router mode.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

For IPv6 multicast BGP (MBGP) distance, the distance assigned is used in reverse path forwarding (RPF) lookup. Use the **show ipv6 rpf** command to display the distance assigned.

Caution Changing the administrative distance of BGP internal routes is considered dangerous to the system and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

Examples

In the following address family configuration mode example, internal routes are known to be preferable to those learned through Interior Gateway Protocol (IGP), so the IPv6 BGP administrative distance values are set accordingly:

```
router bgp 65001
 neighbor 2001:0DB8::1 remote-as 65002
 address-family ipv6
 distance bgp 20 20 200
 neighbor 2001:0DB8::1 activate
 exit-address-family
```

Related Commands

Command	Description
show ipv6 rpf	Displays RPF information for a given unicast host address and prefix.

distribute-list prefix-list (IPv6 EIGRP)

To apply a prefix list to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list**command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name*
no distribute-list prefix-list *list-name*

Syntax Description

list-name	Name of a prefix list. The list defines which EIGRP for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.

Command Default

Prefix lists are not applied to EIGRP for IPv6 routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The prefix list is applied to routing updates received or sent on all interfaces.

Examples

The following example applies prefix list list1 to routes received and sent on all interfaces:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# distribute-list prefix-list list1
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (IPv6 OSPF)

To apply a prefix list to Open Shortest Path First (OSPF) for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list**command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}
no distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}

Syntax Description

list-name	Name of a prefix list. The list defines which OSPF for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.
out	Restricts which prefixes OSPF for IPv6 will identify to the other protocol.
routing-process	Name of a specific routing process. Valid entries for this value are **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip,** or **static**.
as-number	(Optional) Autonomous system number, required for use with Border Gateway Protocol (BGP) and Routing Information Protocol (RIP).

Command Default

Prefix lists are not applied to OSPF for IPv6 routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Service Routers.
12.2(33) SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was modified. The **eigrp** and **ospf** keywords were added for the *routing process* argument.
15.1(2)T	This command was modified. The **eigrp** and **ospf** keywords were added for the *routing process* argument.

Usage Guidelines

If no interface is specified when the **in** keyword is used, the prefix list is applied to routing updates received on all interfaces.

Examples

The following example applies prefix list PL1 to routes received on Ethernet interface 0/0, and applies prefix list PL2 to advertised routes that came from process bgp 65:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# distribute-list prefix-list PL1 in Ethernet0/0
Router(config-router)# distribute-list prefix-list PL2 out bgp 65
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (IPv6 RIP)

To apply a prefix list to IPv6 Routing Information Protocol (RIP) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *listname* {**in** | **out**} [*interface-type interface-number*]
no distribute-list prefix-list *listname*

Syntax Description

listname	Name of a prefix list. The list defines which IPv6 RIP networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
out	Applies the prefix list to outgoing routing updates on the specified interface.
interface-type	(Optional) The specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	(Optional) The specified interface number.

Command Default

Prefix lists are not applied to IPv6 RIP routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If no interface is specified, the prefix list is applied to all interfaces.

Examples

The following example applies the prefix list named cisco to IPv6 RIP routing updates that are received on Ethernet interface 0/0:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# distribute-list prefix-list cisco in ethernet 0/0
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (OSPFv3)

To apply a prefix list to Open Shortest Path First version 3 (OSPFv3) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in IPv6 or IPv4 address family configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}
no distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}

Syntax Description

list-name	Name of a prefix list. The list defines which OSPFv3 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.
out	Restricts which prefixes OSPFv3 will identify to the other protocol.
routing-process	Name of a specific routing process. Valid entries for this value are **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip,** or **static**.
as-number	(Optional) Autonomous system number, required for use with Border Gateway Protocol (BGP) and Routing Information Protocol (RIP).

Command Default

Prefix lists are not applied to OSPFv3 routing updates.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If no interface is specified when the **in** keyword is used, the prefix list is applied to routing updates received on all interfaces.

Examples

The following example enters IPv6 address family configuration mode, applies prefix list PL1 to routes received on Ethernet interface 0/0, and applies prefix list PL2 to advertised routes that came from process bgp 65:

```
Router(config-router)# address-family ipv6 unicast

Router(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0
Router(config-router-af)# distribute-list prefix-list PL2 out bgp 65
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*
no dns-server *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

Command	Description
domain-name	Configures a domain name for a DHCP for IPv6 client.
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

domain-name (IPv6)

To configure a domain name for a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client, use the **domain-name**command in DHCPv6 pool configuration mode. To return to the default for this command, use the **no** form of this command.

domain-name *domain-name*
no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCPv6 pool configuration mode (config-dhcp)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the domain-name command in IPv6 configure a domain name for a DHCPv6 client.

Examples

The following example configures a domain name for a DHCPv6 client:

```
Router(config)# ipv6 dhcp pool pool1
Router(cfg-dns-view)# domain-name domainv6
```

drop-unsecure

To drop messages with no or invalid options or an invalid signature, use the **drop-unsecure**command in neighbor discovery (ND) inspection policy configuration mode or or router advertisement (RA) guard policy configuration mode. To disable this function, use the **no** form of this command.

drop-unsecure
no drop-unsecure

Syntax Description

This command has no arguments or keywords.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **drop-unsecure** command drops messages with no or invalid Cryptographically Generated Address (CGA) options or Rivest, Shamir, and Adleman (RSA) signature as per RFC 3971, *Secure Discovery (SeND)*. However, note that messages with an RSA signature or CGA options that do not conform with or are not verified per RFC 3972, *Cryptographically Generated Addresses (CGA)*, are dropped.

Use the **drop-unsecure** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and enables the router to drop messages with invalid CGA options or an invalid RSA signature:

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

enforcement

To set the enforcement level of a destination guard policy, use the **enforcement** command in destination-guard configuration mode.

enforcement {**always** | **stressed**}

Syntax Description

always	Sets the enforcement level to always.
stressed	Sets the enforcement level to forced only when the system is under stress.

Command Default

The enforcement level of a destination guard policy is set to always.

Command Modes

Destination-guard configuration (config-destguard)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Depending on the network architecture, the sources of binding table information, and the degree of change in the system, the binding table may not always have complete information about the node membership of a VLAN. The enforcement level policy element means that systems with authoritative knowledge of the VLAN membership should set the enforcement level to always. Systems with less confidence, or those with a strong desire to avoid inadvertent packet loss, should set the enforcement level to stressed.

Examples

The following example shows how to set the enforcement level to always:

```
Device(config)# ipv6 destination-guard policy destination
Device(config-destguard)# enforcement always
```

Related Commands

Command	Description
ipv6 destination-guard policy	Defines the destination guard policy.

eui-interface

To use the Media Access Control (MAC) address from a specified interface for deriving the IPv6 mobile home address, use the **eui-interface** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

eui-interface *interface-type* *interface-number*
no **eui-interface** *interface-type* *interface-number*

Syntax Description

interface-type interface-number	Interface type and number from which the MAC address is derived.

Command Default

A MAC address is not used to derive the IPv6 mobile home address.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **eui-interface** command to physically connect to the MAC to get the EUI-64 interface ID.

Examples

In the following example, the router derives the EUI-64 interface ID from the specified interface:

```
eui-interface Ethernet 0/0
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

evaluate (IPv6)

To nest an IPv6 reflexive access list within an IPv6 access list, use the **evaluate** (IPv6) command in IPv6 access list configuration mode. To remove the nested IPv6 reflexive access list from the IPv6 access list, use the **no** form of this command.

evaluate *access-list-name* [**sequence** *value*]
no evaluate *access-list-name* [**sequence** *value*]

Syntax Description

access-list-name	The name of the IPv6 reflexive access list that you want evaluated for IPv6 traffic entering your internal network. This is the name defined in the **permit** (IPv6) command. Names cannot contain a space or quotation mark, or begin with a numeric.
sequence *value*	(Optional) Specifies the sequence number for the IPv6 reflexive access list. The acceptable range is from 1 to 4294967295.

Command Default

IPv6 reflexive access lists are not evaluated.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

This command is used to achieve IPv6 reflexive filtering, a form of session filtering.

Before this command will work, you must define the IPv6 reflexive access list using the **permit** (IPv6) command.

This command nests an IPv6 reflexive access list within an IPv6 access control list (ACL).

If you are configuring an IPv6 reflexive access list for an external interface, the IPv6 ACL should be one that is applied to inbound traffic. If you are configuring IPv6 reflexive access lists for an internal interface, the IPv6 ACL should be one that is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the IPv6 reflexive access list.)

This command allows IPv6 traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IPv6 ACL; the entry "points" to the IPv6 reflexive access list to be evaluated.

As with all IPv6 ACL entries, the order of entries is important. Normally, when a packet is evaluated against entries in an IPv6 ACL, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With an IPv6 reflexive access list nested in an IPv6 ACL, the IPv6 ACL entries are evaluated sequentially up to the nested entry, then the IPv6 reflexive access list entries are evaluated sequentially, and then the remaining entries in the IPv6 ACL are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

Note IPv6 reflexive access lists do not have any implicit deny or implicit permit statements.

Examples

The **evaluate** command in the following example nests the temporary IPv6 reflexive access lists named TCPTRAFFIC and UDPTRAFFIC in the IPv6 ACL named OUTBOUND. The two reflexive access lists are created dynamically (session filtering is "triggered") when incoming TCP or UDP traffic matches the applicable permit entry in the IPv6 ACL named INBOUND. The OUTBOUND IPv6 ACL uses the temporary TCPTRAFFIC or UDPTRAFFIC access list to match (evaluate) outgoing TCP or UDP traffic related to the triggered session. The TCPTRAFFIC and UDPTRAFFIC lists time out automatically when no IPv6 packets match the permit statement that triggered the session (the creation of the temporary reflexive access list).

Note The order of IPv6 reflexive access list entries is not important because only permit statements are allowed in IPv6 reflexive access lists and reflexive access lists do not have any implicit conditions. The OUTBOUND IPv6 ACL simply evaluates the UDPTRAFFIC reflexive access list first and, if there were no matches, the TCPTRAFFIC reflexive access list second. Refer to the **permit** command for more information on configuring IPv6 reflexive access lists.

```
ipv6 access-list INBOUND
  permit tcp any any eq bgp reflect TCPTRAFFIC
  permit tcp any any eq telnet reflect TCPTRAFFIC
  permit udp any any reflect UDPTRAFFIC
ipv6 access-list OUTBOUND
  evaluate UDPTRAFFIC
  evaluate TCPTRAFFIC
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

event-log (OSPFv3)

To enable Open Shortest Path First version 3 (OSPFv3) event logging in an IPv4 OSPFv3 process, use the **event-log** command in OSPFv3 router configuration mode. To disable this feature, use the **no** version of the command.

event-log [{**one-shot** | **pause** | **size** *number-of-events*}]

Syntax Description

one-shot	(Optional) Disables OSPFv3 event logging when the log buffer becomes full.
pause	(Optional) Pauses the event logging function.
size *number-of-events*	(Optional) Configures the maximum number of events stored in the event log. The range is from 1 through 65534.

Command Default

Event logging is not enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

<<Need some guidelines>>

Examples

The following examples show how to enable event logging in an IPv4 OSPFv3 process:

```
Router(config)# router ospfv3 1
Router(config-router)# event-log
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

explicit-prefix

To register IPv6 prefixes connected to the IPv6 mobile router, use the **explicit-prefix**command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

explicit-prefix
no explicit-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No IPv6 prefixes are specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The mobile router presents a list of prefixes to the home agent as part of the binding update procedure. If the home agent determines that the mobile router is authorized to use these prefixes, it sends a bind acknowledgment message.

Examples

The following example shows how to register connected IPv6 prefixes:

```
Router(IPv6-mobile-router)# explicit-prefix
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

frame-relay map ipv6

To define the mapping between a destination IPv6 address and the data-link connection identifier (DLCI) used to connect to the destination address, use the **frame-relay map ipv6**command in interface configuration mode. To delete the map entry, use the **no** form of this command.

frame-relay map ipv6 *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
no frame-relay map ipv6 *ipv6-address*

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a permanent virtual circuit (PVC). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dlci	DLCI number used to connect to the specified protocol address on the interface. The acceptable range is from 16 to 1007.
broadcast	(Optional) Forwards IPv6 multicast packets to this address when multicast is not enabled (see the **frame-relay multicast-dlci** command for more information about multicasts). **Note** IPv6 supports multicast packets; broadcast packets are not supported.
cisco	(Optional) Cisco encapsulation method.
ietf	(Optional) Internet Engineering Task Force (IETF) Frame Relay encapsulation method. Used when the router or access server is connected to the equipment of another vendor across a Frame Relay network.
payload-compression	(Optional) Enables payload compression.
packet-by-packet	(Optional) Packet-by-packet payload compression using the Stacker method.
frf9 stac	(Optional) FRF.9 compression using the Stacker method: • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the Versatile Interface Processor (VIP2) (distributed compression). • If the second-generation VIP2 is not available, compression is performed in the main processor of the router (software compression).
data-stream stac	(Optional) Data-stream compression using the Stacker method: • If the router contains a CSA, compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the main processor of the router (software compression).

hardware-options	(Optional) Choose one of the following hardware options: • **distributed** --Specifies that compression is implemented in the software that is installed in the VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression. • **software** -- Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router. • **csa** *csa-number* -- Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.

Command Default

No mapping is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **frame-relay map ipv6**command is similar to the **frame-relay map** command, except that it is IPv6-specific.

Many DLCIs can be known by a router or access server and can send data to many different places, but they are all multiplexed over one physical link. The Frame Relay map defines the logical connection between a specific protocol and address pair and the correct DLCI.

The optional **ietf** and **cisco** keywords allow flexibility in the configuration. If no keywords are specified, the map inherits the attributes set with the **encapsulation frame-relay** command. You can also use the encapsulation options to specify that, for example, all interfaces use IETF encapsulation except one, which needs the original Cisco encapsulation method and can be configured through use of the **cisco** keyword with the **frame-relay map ipv6**command.

Data-stream compression is supported on interfaces and virtual circuits (VCs) using Cisco proprietary encapsulation. When the **data-stream stac** keywords are specified, Cisco encapsulation is automatically enabled. FRF.9 compression is supported on IETF-encapsulated VCs and interfaces. When the **frf9 stac**keywords are specified, IETF encapsulation is automatically enabled.

Packet-by-packet compression is Cisco-proprietary and will not interoperate with routers of other manufacturers.

You can disable payload compression by entering the **no frame-relay map ipv6 payload-compression** command and then entering the **frame-relay map ipv6**command again with one of the other encapsulation keywords (**ietf** or **cisco**).

Use the **frame-relay map ipv6**command to enable or disable payload compression on multipoint interfaces. Use the **frame-relay payload-compression**command to enable or disable payload compression on point-to-point interfaces.

We recommend that you shut down the interface before changing encapsulation types. Although not required, shutting down the interface ensures that the interface is reset for the new encapsulation.

Examples

In the following example, three nodes named Cisco A, Cisco B, and Cisco C make up a fully meshed network. Each node is configured with two PVCs, which provide an individual connection to each of the other two nodes. Each PVC is configured on a different point-to-point subinterface, which creates three unique IPv6 networks (2001:0DB8:2222:1017::/64, 2001:0DB8:2222:1018::/64, and 2001:0DB8:2222:1019::/64). Therefore, the mappings between the IPv6 addresses of each node and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses are implicit (no additional mappings are required).

Note Given that each PVC in the following example is configured on a different point-to-point subinterface, the configuration in the following example can also be used in a network that is not fully meshed. Additionally, configuring each PVC on a different point-to-point subinterface can help simplify your routing protocol configuration. However, the configuration in the following example requires more than one IPv6 network, whereas configuring each PVC on point-to-multipoint interfaces requires only one IPv6 network.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
!
interface Serial3.17 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1017::46/64
 frame-relay interface-dlci 17
!
interface Serial3.19 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1019::46/64
 frame-relay interface-dlci 19
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
!
interface Serial5.17 point-to-point
 description to Cisco A
```

```
 ipv6 address 2001:0DB8:2222:1017::73/64
 frame-relay interface-dlci 17
!
interface Serial5.18 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1018::73/64
 frame-relay interface-dlci 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
!
interface Serial0.18 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1018::72/64
 frame-relay interface-dlci 18
!
interface Serial0.19 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1019::72/64
 frame-relay interface-dlci 19
```

In the following example, the same three nodes (Cisco A, Cisco B, and Cisco C) from the previous example make up a fully meshed network and each node is configured with two PVCs (which provide an individual connection to each of the other two nodes). However, the two PVCs on each node in the following example are configured on a single interface (serial 3, serial 5, and serial 10, respectively), which makes each interface a point-to-multipoint interface. Therefore, explicit mappings are required between the link-local and global IPv6 addresses of each interface on all three nodes and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::46/64
 frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::72 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 17
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::73/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 17
 frame-relay map ipv6 2001:0DB8:2222:1044::72 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::72/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast
 frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 18
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay payload-compress	Enables Stacker payload compression on a specified point-to-point interface or subinterface.

glbp ipv6

To activate the Gateway Load Balancing Protocol (GLBP) in IPv6, use the **glbp ipv6**command in interface configuration mode. To disable GLBP, use the **no**form of this command.

glbp *group* **ipv6** [{*ipv6-address* | **autoconfig**}]
no glbp *group* **ipv6** [{*ipv6-address* | **autoconfig**}]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
ip-address	(Optional) Virtual IPv6 address for the GLBP group. The IPv6 address must be in the same subnet as the interface IPv6 address.
autoconfig	(Optional) Indicates a default IPv6 address can be created based on a MAC address.

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **glbp ipv6** command activates GLBP on the configured interface. If an IPv6 address is specified, that address is used as the designated virtual IPv6 address for the GLBP group. If no IPv6 address is specified, the designated address is learned from another router configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one router on the cable must have been configured with the designated address. A router must be configured with, or have learned, the virtual IPv6 address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ipv6** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IPv6 address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Examples

The following example enables GLBP on an IPv6 configured interface:

```
Router(config-if)# glbp ipv6
```

Related Commands

Command	Description
glbp ip	Activates the GLBP in IPv4.

Command	Description
show glbp	Displays GLBP information.

graceful-restart

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-capable router, use the **graceful-restart**command in OSPF router configuration mode. To disable graceful restart, use the **no** form of this command.

graceful-restart [**restart-interval** *interval*]
no graceful-restart

Syntax Description

restart-interval *interval*	(Optional) Graceful-restart interval in seconds. The range is from 1 to 1800, and the default is 120.

Command Default

The GR feature is not enabled on GR-capable routers.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **graceful-restart** command can be enabled only on GR-capable routers.

Examples

The following examples enables graceful restart mode on a GR-capable router in IPv6 and IPv4:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restar
```

The following examples enables graceful restart mode on a GR-capable router in IPv6 only:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPFv3 graceful restart feature on a GR-aware router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

graceful-restart helper

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-aware router, use the **graceful-restart helper**command in OSPFv3 router configuration mode. To reset the router to its default, use the **no** form of this command.

graceful-restart helper {**disable** | **strict-lsa-checking**}
no graceful-restart helper

Syntax Description

disable	Disables graceful-restart-aware mode.
strict-lsa-checking	Enables graceful restart-helper mode with strict link-state advertisement (LSA) checking.

Command Default

Graceful restart-aware mode is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
15.1(1)SY	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.

Usage Guidelines

GR-helper mode is configurable on both GR-aware and GR-capable routers; however, GR-aware routers can use only the **graceful-restart helper** command.

The **strict-lsa-checking** keyword indicates whether an OSPFv3 GR-aware router should terminate the helper function when there is a change to an LSA that would be flooded to the restarting router or when there is a changed LSA on the restarting router's retransmission list when graceful restart is initiated.

Examples

The following example enables GR-helper mode with strict LSA checking:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart helper strict-lsa-checking
```

The following example shows how to enable GR-helper mode in an OSPFv3 IPv4 instance:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restart helper
```

Related Commands

Command	Description
graceful-restart	Enables the OSPFv3 GR feature on a graceful-restart-capable router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

hardware statistics

To enable the collection of hardware statistics, use the **hardware statistics**command in IPv6or IPv4 access-list configuration mode. To disable this feature, use the **no** form of this command.

hardware statistics
no hardware statistics

Syntax Description

This commands has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

IPv6 access-list configuration (config-ipv6-acl)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The hardware statistics command affects only global access-list (ACL) counters.

Examples

The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```

home-address

To specify the mobile router home address using an IPv6 address or interface identifier, use the **home-address**command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-address {**home-network***ipv6-address-identifier* | **interface**}
no **home-address**

Syntax Description

home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6-address-identifier	The IPv6 home address identifier.
interface	Specifies the interface to use to identify the home address.

Command Default

No IPv6 home address is specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **home-address**command allows you to specify the IPv6 home address. When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

home-network

To specify the home network's IPv6 prefix on the mobile router, use the **home-network**command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-network *ipv6-prefix*
no home-network

Syntax Description

ipv6-prefix	The IPv6 prefix of the home network.

Command Default

The IPv6 home network prefix is not specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Users can configure up to 10 home-network entries, and they are used in order of priority. The prefix identifies the home network of the mobile router and is used to discover when the mobile router is at home.

When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

The command syntax sorts the home networks by priority. The default priority is 128. The home networks will be tried from the smaller to the higher value and, for a same priority, the addresses without the discover keyword are tried first.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-address	Specifies the mobile router home address using an IPv6 address or interface identifier.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in RA guard policy configuration mode.

hop-limit {**maximum** | **minimum** } *limit*

Syntax Description

maximum *limit*	Verifies that the hop-count limit is lower than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

host group

To create a host group configuration in IPv6 Mobile, use the **host group**command in home agent configuration mode. To remove a host configuration, use the **no** form of this command.

host group *profile-name*
no host group *profile-name*

Syntax Description

profile-name	Specifies a name for the host group.

Command Default

No IPv6 Mobile host configurations exist.

Command Modes

Home agent configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **host group** command creates an IPv6 Mobile home-agent host configuration with a given profile name. Multiple instances with different profile names can be created and used.

Do not configure two separate groups with the same IPv6 address. For example, host group group1 and host group group2 cannot both be configured with the same IPv6 address of baba::1.

Examples

In the following example, the user enters home agent configuration mode and creates a host group named group1:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)# host group group1
```

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 Mobile node.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the **identity**command in IKEv2 keyring peer configuration mode. To remove the identity, use the **no** form of this command.

identity {**address**{*ipv4-addressipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *domain-name*}
no identity {**address**{*ipv4-addressipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address to identify the peer.
fqdn domain *domain-name*	Uses the Fully Qualified Domain Name (FQDN) to identify the peer.
email domain*domain-name*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietary types to identify the peer.

Command Default

Identity types are not specified to a peer.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.3(3)M	This command was modified. The **domain** *domain-name* keyword-argument pair was added.

Usage Guidelines

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an e-mail ID, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session, and the initiator looks up keys during session startup.

Examples

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 or IPv6 address or the range of the peers in an IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

identity local

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the **identity local**command in IKEv2 profile configuration mode. To remove the identity, use the **no** form of this command.

identity local {**address**{*ipv4-addressipv6-address*} | **dn** | **fqdn** *fqdn-string* | **email** *e-mail-string* | **key-id** *opaque-string*}
no identity

Syntax Description

address *{ipv4-address | ipv6-address}*	Uses the IPv4 or IPv6 address as the local identity.
dn	Uses the distinguished name as the local identity.
fqdn *fqdn-string*	Uses the Fully Qualified Domain Name (FQDN) as the local identity.
email *email-string*	Uses the e-mail ID as the local identity.
key-id *opaque-string*	Uses the proprietary type opaque string as the local identity.

Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6). If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.

Note You can configure one local IKEv2 identity type for a profile.

Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
```

```
Router(config-ikev2-profile)# identity local address 10.0.0.1
The following example shows how to specify an IPv6 address as the local IKEv2 identity:
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

import dns-server

To import the Domain Name System (DNS) recursive name server option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import dns-server**command in IPv6 DHCP pool configuration mode. To remove the available DNS recursive name server list, use the **no** form of this command.

import dns-server
no import dns-server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS recursive name server list is not imported to a client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The DNS recursive name server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.

The DNS recursive name server list option code is 23. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a list of available DNS recursive name servers to a client:

```
Router(config-dhcp)# import dns-server
```

Related Commands

Command	Description
import domain-name	Imports the domain search list option to a DHCP for IPv6 client.

import domain-name

To import the domain name search list option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name search list, use the **no** form of this command.

import domain-name
no import domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

The domain search list is not imported to the client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The domain name search list option specifies the domain search list the client is to use when resolving hostnames with DNS.

The domain name search list option code is 24. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a domain search list to the client:

```
Router(config-dhcp)# import domain-name
```

Related Commands

Command	Description
import dns-server	Imports the DNS recursive name server option to a DHCP for IPv6 client.

import information refresh

To import the information refresh time option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

import information refresh
no import information refresh

Syntax Description

This command has no arguments or keywords.

Command Default

The information refresh time option is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCP for IPv6. It is used only in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the information refresh time:

```
import information refresh
```

Related Commands

Command	Description
information refresh	Specifies the information refresh time to be sent to the client.

import nis address

To import the network information service (NIS) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nis address
no import nis address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS servers option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server’s preference.

The NIS servers option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS address of an IPv6 server:

```
import nis address
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client’s NIS domain name information to the client.

import nis domain-name

To import the network information service (NIS) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nis domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS domain name is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client.

The NIS domain name option code is 29.

Examples

The following example shows how to import a client's NIS domain name:

```
import nis domain-name
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nisp address

To import the network information service plus (NIS+) servers option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nisp address
no import nisp address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ address of an IPv6 server:

```
import nisp address
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name
no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import sip address

To import the Session Initiation Protocol (SIP) server IPv6 address list option to the outbound SIP proxy server, use the **import sip address**command in IPv6 DHCP pool configuration mode. To remove the SIP server IPv6 address list, use the **no** form of this command.

import sip address
no import sip address

Syntax Description

This command has no arguments or keywords.

Command Default

SIP IPv6 address list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server IPv6 address list option specifies a list of IPv6 addresses that indicate SIP outbound proxy servers available to the client. Servers must be listed in order of preference.

The SIP server IPv6 address list option code is 22. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server IPv6 address list to the client:

```
Router(config-dhcp)# import
 sip address
```

Related Commands

Command	Description
import sip domain-name	Imports a SIP server domain-name list option to the outbound SIP proxy server.

import sip domain-name

To import a Session Initiation Protocol (SIP) server domain-name list option to the outbound SIP proxy server, use the **import sip domain-name**command in IPv6 DHCP pool configuration mode. To remove the SIP server domain-name list, use the **no** form of this command.

import sip domain-name
no import sip domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

SIP domain-name list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server domain-name list option contains the domain names of the SIP outbound proxy servers. Domain names must be listed in order of preference. The option may contain multiple domain names, but the client must try the records in the order listed. The client resolves the subsequent domain names only if attempts to contact the first one failed or yielded no common transport protocols between client and server or denoted a domain administratively prohibited by client policy.

The SIP server domain-name list option code is 21. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server domain-name list to the client:

```
Router(config-dhcp)# import sip domain-name
```

Related Commands

Command	Description
import sip address	Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

import sntp address

To import the Simple Network Time Protocol (SNTP) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import sntp address** command in IPv6 DHCP pool configuration mode. To remove the SNTP server address, use the **no** form of the command.

import sntp address *ipv6-address*
no import sntp address *ipv6-address*

Syntax Description

ipv6-address	(Optional) The IPv6 address for SNTP. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No SNTP server address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The SNTP address option can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the SNTP server address:

```
import sntp address
```

Related Commands

Command	Description
sntp address	Specifies the SNTP server to be sent to the client.

information refresh

To specify the information refresh time to be sent to the client, use the **information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

information refresh {*days* [*hours minutes*] | **infinity**}
no information refresh {*days* [*hours minutes*] | **infinity**}

Syntax Description

days	Refresh time specified in number of days. The default is 0 0 86400, which equals 24 hours.
hours	(Optional) Refresh time specified in number of hours.
minutes	(Optional) Refresh time specified in number of minutes. The minimum refresh time that can be used is 0 0 600, which is 10 minutes.
infinity	Sets the IPv6 value of 0xffffffff used to configure the information refresh time to infinity.

Command Default

Information refresh information is not sent to the client. The client refreshes every 24 hours if no refresh information is sent.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies the maximum time a client should wait before refreshing information retrieved from DHCP for IPv6. It is only used in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The maximum value for the information refresh period on the DHCP for IPv6 client is 7 days. The maximum value is not configurable.

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the information refresh time to be 1 day, 1 hour, and 1 second:

```
information refresh 1 1 1
```

Related Commands

Command	Description
import information refresh	Imports the information refresh time option to a DHCP for IPv6 client.

IPv6 Commands: ipv6 a to ipv6 g

ipv6 access-class

To filter incoming and outgoing connections to and from the router based on an IPv6 access list, use the **ipv6 access-class**command in line configuration mode. To disable the filtering of incoming and outgoing connections to the router, use the **no** form of this command.

ipv6 access-class *ipv6-access-list-name* {**in** | **out**}
no ipv6 access-class

Syntax Description

ipv6-access-list-name	Name of an IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
in	Filters incoming IPv6 connections.
out	Filters outgoing IPv6 connections.

Command Default

The filtering of incoming and outgoing connections to and from the router is not enabled.

Command Modes

Line configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

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

Identical restrictions should be set on all the virtual terminal lines because a user can connect to any of them.

The incoming connection source address is used to match against the access list source prefix. The router address on the received interface is used to match against the access list destination prefix.

IPv6 access control list (ACL) matches are made using TCP; an ACL permit match using IPv6 or TCP is required to allow access to a router.

Examples

The following example filters incoming connections on virtual terminal lines 0 to 4 of the router based on the IPv6 access list named cisco:

```
ipv6 access-list cisco
 permit ipv6 host 2001:0DB8:0:4::2/128 any
line vty 0 4
 ipv6 access-class cisco in
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 access-list

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

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

Syntax Description

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

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: **permit**, **deny,** *source-ipv6-prefix* / *prefix-length*, **any**, *destination-ipv6-prefix* / *prefix-length*, **priority**. See the "Usage Guidelines" section for more details.
12.2(13)T	Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: **permit**, **deny,** *source-ipv6-prefix* / *prefix-length*, **any**, *destination-ipv6-prefix* / *prefix-length*, **priority**. See the "Usage Guidelines" section for more details.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	Duplicate remark statements can no longer be configured from the IPv6 access control list.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, standard IPv6 access control list (ACL) functionality is used for basic traffic filtering functions--traffic filtering is based on source and destination addresses, inbound and outbound to a specific interface, and with an implicit deny statement at the end of each access list (functionality similar to standard ACLs in IPv4). IPv6 ACLs are defined and their deny and permit conditions are set by using the **ipv6 access-list**command with the **deny** and **permit** keywords in global configuration mode.

In Cisco IOS Release 12.0(23)S or later releases, the standard IPv6 ACL functionality is extended to support--in addition to traffic filtering based on source and destination addresses--filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4). IPv6 ACLs are defined by using the **ipv6 access-list**command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit**commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list**command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

Note IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

In Cisco IOS Release 12.0(23)S or later releases, and 12.2(11)S or later releases, for backward compatibility, the **ipv6 access-list**command with the **deny** and **permit** keywords in global configuration mode is still supported; however, an IPv6 ACL defined with deny and permit conditions in global configuration mode is translated to IPv6 access list configuration mode.

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

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

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

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

Note An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

Note When using this command to modify an ACL that is already associated with a bootstrap router (BSR) candidate rendezvous point (RP) (see the **ipv6 pim bsr candidate rp** command) or a static RP (see the **ipv6 pim rp-address** command), any added address ranges that overlap the PIM SSM group address range (FF3x::/96) are ignored. A warning message is generated and the overlapping address ranges are added to the ACL, but they have no effect on the operation of the configured BSR candidate RP or static RP commands.

In Cisco IOS Release 12.2(33)SXH and subsequent Cisco IOS SX releases, duplicate remark statements can no longer be configured from the IPv6 access control list. Because each remark statement is a separate entity, each one is required to be unique.

Examples

The following example is from a device running Cisco IOS Release 12.0(23)S or later releases. The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example is from a device running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S. The example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

If the same configuration was entered on a device running Cisco IOS Release 12.0(23)S or later releases, the configuration would be translated into IPv6 access list configuration mode as follows:

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any
```

```
interface ethernet 0
 ipv6 traffic-filter list2 out
```

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

Note IPv6 ACLs defined on a device running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S that rely on the implicit deny condition or specify a **deny any any** statement to filter traffic should contain **permit** statements for link-local and multicast addresses to avoid the filtering of protocol packets (for example, packets associated with the neighbor discovery protocol). Additionally, IPv6 ACLs that use **deny** statements to filter traffic should use a **permit any any** statement as the last statement in the list.

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

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-class	Filters incoming and outgoing connections to and from the device based on an IPv6 access list.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
ipv6 pim rp-address	Configure the address of a PIM RP for a particular group range.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 access-list log-update threshold

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

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

Syntax Description

value	Specifies the number of updates that are logged for every IPv6 access list configured on the router. The acceptable range is from 0 to 2147483647.

Command Default

The default is 2147483647 updates.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

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

Examples

The following example configures a log threshold of ten updates for every IPv6 access list configured on the router.

```
ipv6 access-list log-update threshold 10
```

Related Commands

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

ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, 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* | *prefix-name sub-bits/prefix-length*}
no ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
prefix-name	A general prefix, which specifies the leading bits of the network to be configured on the interface.
sub-bits	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument. The *sub-bits*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series devices.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

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

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

Related Commands

Command	Description
ipv6 address anycast	Configures an IPv6 anycast address and enables IPv6 processing on an interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 address autoconfig	Removes all IPv6 addresses from an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address anycast

To configure an IPv6 anycast address and enable IPv6 processing on an interface, use the **ipv6 address anycast**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* **anycast**
no ipv6 address [*ip6-prefix/prefix-length* **anycast**]

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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

Examples

The following example shows how to enable IPv6 processing on the interface, assign the prefix 2001:0DB8:1:1::/64 to the interface, and configure the IPv6 anycast address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE:

```
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address autoconfig [**default**]
no ipv6 address autoconfig

Syntax Description

default	(Optional) If a default device is selected on this interface, the **default** keyword causes a default route to be installed using that default device. The **default** keyword can be specified only on one interface.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address autoconfig** command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement (RA) messages.

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

Examples

The following example assigns the IPv6 address automatically:

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp [**rapid-commit**]
no ipv6 address dhcp

Syntax Description

rapid-commit	(Optional) Allows the two-message exchange method for address assignment.

Command Default

No IPv6 addresses are acquired from the DHCPv6 server.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address dhcp** interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

Examples

The following example shows how to acquire an IPv6 address and enable the rapid-commit option:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** command in privileged EXEC mode.

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCPv6 interface information.

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

ipv6 address dhcp client request vendor
no ipv6 address dhcp client request vendor

Syntax Description

vendor	Requests the vendor-specific options.

Command Default

IPv6 clients are not configured to request an option from DHCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **ipv6 address dhcp client request vendor** command to request a vendor-specific option. When this command is enabled, the IPv6 client can request a vendor-specific option only when an IPv6 address is acquired from DHCP. If you enter the command after the interface has acquired an IPv6 address, the IPv6 client cannot request a vendor-specific option until the next time the client acquires an IPv6 address from DHCP.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp client request vendor
```

Related Commands

Command	Description
ipv6 address dhcp	Acquires an IPv6 address on an interface from the DHCPv6 server.

ipv6 address eui-64

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

ipv6 address *ipv6-prefix/prefix-length* **eui-64**
no ipv6 address [*ip v6-prefix/prefix-length* **eui-64**]

Syntax Description

ipv6-prefix	The IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

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

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

Examples

The following example assigns IPv6 address 2001:0DB8:0:1::/64 to Ethernet interface 0 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address link-local

To configure an IPv6 link-local address for an interface and enable IPv6 processing on the interface, use the **ipv6 address link-local**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address/prefix-length* **link-local** [**cga**]
no ipv6 address [*ipv6-address/prefix-length* **link-local**]

Syntax Description

ipv6-address	The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
link-local	Specifies a link-local address. The *ipv6-address* specified with this command overrides the link-local address that is automatically generated for the interface.
cga	(Optional) Specifies the CGA interface identifier.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(24)T	The **cga** keyword was added
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

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

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

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

Examples

The following example assigns FE80::260:3EFF:FE11:6770 as the link-local address for Ethernet interface 0:

```
interface ethernet 0
 ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 atm-vc

To configure a mapping between a virtual circuit (VC) and the IPv6 address of a system at the far end of that circuit, use the **ipv6 atm-vc** command in map-list configuration mode. To remove the mapping, use the **no** form of this command.

ipv6 *ipv6-address* **atm-vc** *vcd* [**broadcast**]
no ipv6 *ipv6-address* **atm-vc** *vcd* [**broadcast**]

Syntax Description

ipv6-address	The IPv6 address of a system at the far end of the specified virtual circuit. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vcd	The virtual circuit descriptor for the virtual circuit mapped to the specified IPv6 address.
broadcast	(Optional) Specifies that this map entry is used when sending IPv6 multicast packets to the interface (for example, network routing protocol updates).

Command Default

No default behavior or values.

Command Modes

Map-list configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

ATM permanent virtual circuits (PVCs) can be configured in the following modes:

- Nonbroadcast multiaccess (NBMA) mode--A neighbor is mapped to a PVC. ATM point-to-multipoint PVCs are configured using static maps. The ipv6 atm-vc command utilizes static maps.
- Point-to point-mode--Each PVC is given a subinterface and is configured as a standard point-to-point link.

Note We recommend configuring ATM PVCs in point-to-point mode.

Examples

The following example maps neighbor 2001:0DB8::5 to ATM point-to-multipoint PVC 1, virtual path identifier (VPI) 3, and virtual channel identifier (VCI) 5:

```
Router(config)# interface atm 1/0
Router(config-if)# atm pvc 1 3 5 aal5snap
Router(config-if)# map-group cisco
Router(config)# map-list cisco
Router(config-map-list)# ipv6 2001:0DB8::5 atm-vc 1
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **ipv6 authentication key-chain eigrp**command in interface configuration mode. To disable authentication of EIGRP for IPv6 packets, use the **no** form of this command.

ipv6 authentication key-chain eigrp *as-number key-chain*
no ipv6 authentication key-chain eigrp *as-number key-chain*

Syntax Description

as-number	Autonomous system number.
key-chain	Name of the authentication key chain.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 route authentication provides Message Digest 5 (MD5) authentication of routing updates from the EIGRP for IPv6 routing protocol. The MD5 keyed digest in each EIGRP for IPv6 packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters.

Examples

The following example enables authentication for EIGRP for IPv6 for AS 1, using a key chain named chain1:

```
Router(config-if)# ipv6 authentication key-chain eigrp 1 chain1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.

Command	Description
ipv6 authentication mode eigrp	Specifies the type of authentication used in EIGRP for IPv6 packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets for IPv6, use the **ipv6 authentication mode eigrp**command in interface configuration mode. To disable the type of authentication, use the **no** form of this command.

ipv6 authentication mode eigrp *as-number* **md5**
no ipv6 authentication mode eigrp *as-number* **md5**

Syntax Description

as-number	Autonomous system number.
md5	Specifies keyed message digest 5 (MD5) authentication.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **ipv6 authentication mode eigrp**command to configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP for IPv6 packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP for IPv6 packets in autonomous system 1:

```
Router(config-if)# ipv6 authentication mode eigrp 1 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.

Command	Description
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on an interface, use the **ipv6 bandwidth-percent eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 bandwidth-percent eigrp *as-number percent*
no ipv6 bandwidth-percent eigrp *as-number percent*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that EIGRP for IPv6 may use.

Command Default

Percentage of bandwidth used is 50 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 uses as much as 50 percent of the bandwidth of a link, as defined by the **bandwidth** command. The ipv6 bandwidth-percent eigrp command may be used if some other fraction of the bandwidth is desired.

Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows EIGRP for IPv6 to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 1:

```
interface serial 0
 bandwidth 56
 ipv6 bandwidth-percent eigrp 1 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

ipv6 cef

To enable Cisco Express Forwarding for IPv6, use the **ipv6 cef** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef
no ipv6 cef

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding for IPv6 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 cef** command is similar to the **ip cef** command, except that it is IPv6-specific.

The **ipv6 cef** command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed Cisco Express Forwarding for IPv6 mode.

Note The **ipv6 cef**command is not supported in interface configuration mode.

Note Some distributed architecture platforms, such as the Cisco 7500 series routers, support both Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6. When Cisco Express Forwarding for IPv6 is configured on distributed platforms, Cisco Express Forwarding switching is performed by the Route Processor (RP).

Note You must enable Cisco Express Forwarding for IPv4 by using the **ip cef** global configuration command before enabling Cisco Express Forwarding for IPv6 by using the **ipv6 cef** global configuration command.

Cisco Express Forwarding for IPv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as Cisco Express Forwarding for IPv4. Cisco Express Forwarding for IPv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables standard Cisco Express Forwarding for IPv4 operation and then standard Cisco Express Forwarding for IPv6 operation globally on the router.

```
ip cef
ipv6 cef
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
ipv6 cef accounting	Enables Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting.
ipv6 cef distributed	Enables distributed Cisco Express Forwarding for IPv6.
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef accounting

To enable Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting, use the **ipv6 cef accounting**command in global configuration mode or interface configuration mode. To disable Cisco Express Forwarding for IPv6 network accounting, use the **no**form of this command.

ipv6 cef accounting *accounting-types*
no ipv6 cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode
ipv6 cef accounting non-recursive {**external** | **internal**}
no ipv6 cef accounting non-recursive {**external** | **internal**}

Syntax Description

accounting-types	The *accounting-types* argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once. • **load-balance-hash** --Enables load balancing hash bucket counters. • **non-recursive** --Enables accounting through nonrecursive prefixes. • **per-prefix** --Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix). • **prefix-length** --Enables accounting through prefix length.
non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode after another keyword is entered. See the *accounting-types* argument.
external	Counts input traffic in the nonrecursive external bin.
internal	Counts input traffic in the nonrecursive internal bin.

Command Default

Cisco Express Forwarding for IPv6 network accounting is disabled by default.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **non-recursive**and **load-balance-hash**keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 cef accounting**command is similar to the **ip cef accounting**command, except that it is IPv6-specific.

Configuring Cisco Express Forwarding for IPv6 network accounting enables you to collect statistics on Cisco Express Forwarding for IPv6 traffic patterns in your network.

When you enable network accounting for Cisco Express Forwarding for IPv6 by using the **ipv6 cef accounting**command in global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding for IPv6 mode is enabled and at the line cards when distributed Cisco Express Forwarding for IPv6 mode is enabled. You can then display the collected accounting information using the **show ipv6 cef** EXEC command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode after you enter another keyword on the **ipv6 cef accounting**command.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ipv6 cef detail**command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ipv6 cef accounting** command to enable per-hash-bucket counters. Enter the **show ipv6 cef** *prefix* **internal** command to display the per-hash-bucket counters.

Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Router(config)# ipv6 cef accounting non-recursive
```

Related Commands

Command	Description
ip cef accounting	Enable Cisco Express Forwarding network accounting (for IPv4).
show cef	Displays information about packets **forwarded by Cisco Express Forwarding.**

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6, use the **ipv6 cef distributed**command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef distributed
no ipv6 cef distributed

Syntax Description

This command has no arguments or keywords.

Command Default

Distributed Cisco Express Forwarding for IPv6 is disabled on the Cisco 7500 series routers and enabled on the Cisco 12000 series Internet routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 cef distributed**command is similar to the **ip cef distributed**command, except that it is IPv6-specific.

Enabling distributed Cisco Express Forwarding for IPv6 globally on the router by using the **ipv6 cef distributed**in global configuration mode distributes the Cisco Express Forwarding processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.

Note The **ipv6 cef distributed** command is not supported on the Cisco 12000 series Internet routers because distributed Cisco Express Forwarding for IPv6 is enabled by default on this platform.

Note To forward distributed Cisco Express Forwarding for IPv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the **ipv6 unicast-routing** global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.

Note You must enable distributed Cisco Express Forwarding for IPv4 by using the **ip cef distributed**global configuration command before enabling distributed Cisco Express Forwarding for IPv6 by using the **ipv6 cef distributed**global configuration command.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables distributed Cisco Express Forwarding for IPv6 operation:

```
ipv6 cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the **ipv6 cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

ipv6 cef load-sharing algorithm {**original** | **universal** [*id*] | **include-ports** {**source** [*id*] | [**destination**] [*id*] | **source** [*id*] **destination** [*id*] **gtp**}}
no ipv6 cef load-sharing algorithm

Syntax Description

original	Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
universal	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
id	(Optional) Fixed identifier in hexadecimal format.
include-ports source	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
include-ports destination	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
include-ports source destination	Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.
include-ports source destination gtp	Sets the load-balancing algorithm based on the GPRS Tunneling Protocol Tunnel Endpoint Identifier (GTP TEID) for the GTP-U packets. Sets the load-balancing algorithm based on the Layer 4 source and destination ports for the non-GTP-U packets.

Command Default

The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
3.10S	This command is supported in Cisco IOS XE Release 3.10S. The **gtp** keyword was added to the command.

Usage Guidelines

The **ipv6 cef load-sharing algorithm**command is similar to the **ip cef load-sharing algorithm**command, except that it is IPv6-specific.

When the Cisco Express Forwarding for IPv6 load-balancing algorithm is set to universal mode, each router on the network can make a different load-sharing decision for each source-destination address pair.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not load-shared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for IPv6 for Layer-4 source and destination ports:

```
Router(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The router automatically generates fixed IDs for the algorithm.

The following example shows how to enable the IPv6 CEF load-sharing algorithm based on GTP TEID:

```
configure terminal
!
 ipv6 cef load-sharing algorithm include-ports source destination gtp
 exit
```

Related Commands

Command	Description
debug ipv6 cef hash	Displays debug messages for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 load-sharing hash algorithm events.
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).

ipv6 cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **ipv6 cef optimize neighbor resolution**command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **no** form of this command.

ipv6 cef optimize neighbor resolution
no ipv6 cef optimize neighbor resolution

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, Cisco Express Forwarding for IPv6 does not optimize the address resolution of directly connected neighbors.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ipv6 cef optimize neighbor resolution** command is very similar to the **ip cef optimize neighbor resolution** command, except that it is IPv6-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv6.

Examples

The following example shows how to optimize address resolution from Cisco Express Forwarding for IPv6 for directly connected neighbors:

```
Router(config)# ipv6 cef optimize neighbor resolution
```

Related Commands

Command	Description
ip cef optimize neighbor resolution	Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.

ipv6 cga modifier rsakeypair

To generate an IPv6 cryptographically generated address (CGA) modifier for a specified Rivest, Shamir, and Adelman (RSA) key pair, use the **ipv6 cga modifier rsakeypair**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga modifier rsakeypair *key-label* **sec-level** *sec-level-value* [{**max-iterations value** *cga-modifier*}]
no ipv6 cga modifier rsakeypair

Syntax Description

key-label	The name to be used for RSA key pair
sec-level *sec-level-value*	Specifies the security level, which can be a number from 0 through 3. The most secure level is 1.
max-iterations*value*	(Optional) Maximum iteration for modifier generation. The *value* can be a number from 0 through 40000000.
cga-modifier	(Optional) An IPv6 address used as a CGA modifier.

Command Default

No CGA exists for an RSA key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(3)T	The **max-iterations** keyword and *cga-modifier* argument were added.

Usage Guidelines

Use this command to generate the CGA modifier for a specified RSA key pair, which enables the key to be used by Secure Neighbor Discovery (SeND).

Once the RSA key is generated, the modifier must be generated as well, using the **ipv6 cga modifier rsakeypair** command.

A CGA has a security parameter that determines its strength against brute-force attacks. The security level can be either 0 or 1.

Examples

The following example enables the specified key to be used by SeND (that is, generates the modifier):

```
Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair	Generates the CGA modifier for a specified RSA key.

Command	Description
ipv6 cga modifier rsakeypair (interface)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 cga rsakeypair

To bind a Secure Neighbor Discovery (SeND) key to a specified interface, use the **ipv6 cga rsakeypair**command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga rsakeypair *key-label*
no ipv6 cga rsakeypair

Syntax Description

key-label	The name to be used for the Rivest, Shamir, and Adelman (RSA) key pair.

Command Default

A SeND key is not bound to an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The SeND key is used to generate an IPv6 modifier for a specified Rivest, Shamir and Adelman (RSA) key pair. A SeND key must be bound to the interface prior to its being used in the **ipv6 address** command. Use the **ipv6 cga rsakeypair** command to bind a SeND key to a specified interface.

You can then use the **ipv6 address** command to add the Cryptographic Addresses (CGA).

Examples

The following example binds a SeND key to Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.1.1 255.255.255.0
Router(config-if)# ipv6 cga rsakeypair SEND
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair (global configuration)	Generates the CGA modifier for a specified RSA key.
ipv6 cga modifier rsakeypair (interface configuration)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 crypto map

To enable an IPv6 crypto map on an interface, use the **ipv6 crypto map** command in interface configuration mode. To disable, use the **no** form of this command.

ipv6 crypto map *map-name*
no ipv6 crypto map

Syntax Description

map-name	Identifies the crypto map set.

Command Default

No IPv6 crypto maps are enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command differentiates IPv6 and IPv4 crypto maps.

Examples

The following example shows how to enable an IPv6 crypto map on an interface:

```
Router# configure terminal
Router(config
)# interface ethernet 0/0
Router(config-if
)# ipv6 crypto map CM_V4
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry.

ipv6 destination-guard attach-policy

To attach a destination guard policy, use the **ipv6 destination-guard attach-policy** command in VLAN configuration mode or interface configuration mode. To unattach the destination-guard policy, use the **no** form of this command.

ipv6 destination-guard attach-policy [*policy-name*]
no ipv6 destination-guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of the destination guard policy.

Command Default

No destination guard policy is attached.

Command Modes

VLAN configuration (config-vlan-config)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command allows you to attach a destination guard policy to a router or an interface. These policies can be used to filter IPv6 traffic based on the destination address, and block any data traffic from an unknown source.

Examples

The following example shows how to attach a destination guard policy to a router:

```
Device> enable
Device# configure terminal
Device(config)# vlan configuration 1
Device(config-vlan-config)# ipv6 destination-guard attach-policy pol1
```

Related Commands

Command	Description
ipv6 destination-guard policy	Defines the destination guard policy.
show ipv6 destination-guard policy	Displays destination guard information.

ipv6 destination-guard policy

To define a destination guard policy, use the **ipv6 destination-guard policy** command in global configuration mode. To remove the destination guard policy, use the **no** form of this command.

ipv6 destination-guard policy [*policy-name*]
no ipv6 destination-guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of the destination guard policy.

Command Default

No destination guard policy is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command enters destination-guard configuration mode. The destination guard policies can be used to filter IPv6 traffic based on the destination address to block data traffic from an unknown source.

Examples

The following example shows how to define the name of a destination guard policy:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 destination-guard policy policy1
Router(config-destguard)#
```

Related Commands

Command	Description
show ipv6 destination-guard policy	Displays destination guard information.

ipv6 dhcp binding track ppp

To configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to release any bindings associated with a PPP connection when that connection closes, use the **ipv6 dhcp binding track ppp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp

Syntax Description

This command has no arguments or keywords.

Command Default

When a PPP connection closes, the DHCP bindings associated with that connection are not released.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **ipv6 dhcp binding track ppp** command configures DHCP for IPv6 to automatically release any bindings associated with a PPP connection when that connection is closed. The bindings are released automatically to accommodate subsequent new registrations by providing sufficient resource.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using this command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator clears the binding.

Examples

The following example shows how to release the prefix bindings associated with the PPP:

```
Router(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable Dynamic Host Configuration Protocol (DHCP) for IPv6 client information refresh time on a specified interface, use the **ipv6 dhcp client information refresh minimum**command in interface configuration mode. To remove the configured refresh time, use the **no** form of this command.

ipv6 dhcp client information refresh minimum *seconds*
no ipv6 dhcp client information refresh minimum *seconds*

Syntax Description

seconds	The refresh time, in seconds. The minimum value that can be used is 600 seconds.

Command Default

The default is 86,400 seconds (24 hours).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The **ipv6 dhcp client information refresh minimum**command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

Examples

The following example configures an upper limit of 2 hours:

```
ipv6 dhcp client information refresh minimum 7200
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]
no ipv6 dhcp client pd

Syntax Description

prefix-name	IPv6 general prefix name.
hint	An IPv6 prefix sent as a hint.
ipv6-prefix	IPv6 general prefix.
rapid-commit	(Optional) Allow two-message exchange method for prefix delegation.

Command Default

Prefix delegation is disabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Enabling the **ipv6 dhcp client pd**command starts the DHCP for IPv6 client process if this process is not yet running.

The **ipv6 dhcp client pd**command enables request for prefix delegation through the interface on which this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the *ipv6-prefix*argument. Other commands and applications (such as the **ipv6 address** command) can then refer to the prefixes in the general prefix pool.

The **hint** keyword with the *ipv6-prefix* argument enables the configuration of an IPv6 prefix that will be included in DHCP for IPv6 solicit and request messages sent by the DHCP for IPv6 client on the interface as a hint to prefix-delegating routers. Multiple prefixes can be configured by issuing the **ipv6 dhcp client pd hint***ipv6-prefix* command multiple times. The new prefixes will not overwrite old ones.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If it is enabled, the client will include the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

Examples

The following example enables prefix delegation:

```
Router(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Router(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

Related Commands

Command	Description
clear ipv6 dhcp client	Restarts the DHCP for IPv6 client on an interface.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp client vendor-class

The DHCPv6 client, by default, carries the PID (product ID) of the device in option-16. To override this behaviour, use the following command:

ipv6 dhcp client vendor-class [{ **mac-address** | **ascii** | **hex** | **disable** }]

Syntax Description

mac-address	The MAC address of the device.
ascii	The user defined string in ASCII format.
hex	The user defined string in hexadecimal format.
disable	Disables sending option 16 in DHCPv6 messages.

Command Default

By default, option 16 is enabled and the DHCPv6 client carries the PID (Product ID) of device.

Command Modes

Interface configuration mode.

Usage Guidelines

By default DHCPv6 client carries PID of the device in option-16. This default behaviour can be overridden by configuring the **ipv6 dhcp client vendor-class** command.

Examples

The following example enables option-16:

```
Router(config-if)# ipv6 dhcp client ?
information Configure information refresh option
pd Prefix-Delegation
request Request
vendor-class Configure vendor class data, Product ID by default (Option 16)
```

The following configuration example overrides PID with mac-address:

```
Router(config-if)# ipv6 dhcp client vendor-class mac-address
```

Examples

The following configuration example overrides PID with user defined string in the hex format:

```
Router(config-if)# ipv6 dhcp client vendor-class hex aabbcc
```

Examples

The following configuration example overrides PID with user defined string in the ascii format:

```
Router(config-if)# ipv6 dhcp client vendor-class ascii cisco
```

Examples

The following configuration example is used to disable sending option-16 in DHCPv6 messages:

```
Router(config-if)# ipv6 dhcp client vendor-class disable
```

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds*]
no ipv6 dhcp database *agent*

Syntax Description

agent	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
timeout *seconds*	(Optional) How long, in seconds, the router waits for a database transfer.

Command Default

Write-delay default is 300 seconds. Timeout default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **ipv6 dhcp database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, updated when the client renews, rebinds, or confirms the prefix delegation, and deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or administrators enable the clear ipv6 dhcp binding command. These bindings are maintained in RAM and can be saved to permanent storage using the *agent* argument so that the information about configuration such as prefixes assigned to clients is not lost after a system reload or power down. The bindings are stored as text records for easy maintenance.

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host such as an FTP server or a local file system such as NVRAM.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are terminated. By default, the DHCP for IPv6 server waits 300 seconds before terminating a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP:

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in bootflash:

```
ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 server binding table
show ipv6 dhcp database	Displays DHCP for IPv6 binding database agent information.

ipv6 dhcp debug redundancy

To display debugging output for IPv6 DHCP high availability (HA) processing, use the **ipv6 dhcp debug redundancy**command in privileged EXEC mode. To disable debugging output, use the no form of this command.

ipv6 dhcp debug redundancy
no ipv6 dhcp debug redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp debug redundancy** command to display stateful switchover (SSO) state transitions and errors.

Examples

The following example enables IPv6 DHCP redundancy debugging:

```
Router# ipv6 dhcp debug redundancy
```

ipv6 dhcp framed password

To assign a framed prefix when using a RADIUS server, use the **ipv6 dhcp framed password**command in interface configuration mode. To remove the framed prefix, use the **no** form of this command.

ipv6 dhcp framed password *password*
no ipv6 dhcp framed password

Syntax Description

password	Password to be used with the RADIUS server.

Command Default

No framed prefix is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The ipv6 dhcp framed password command enables a user to request a framed prefix of a RADIUS server. When a PPPoE client requests a prefix from a network using the framed-prefix system, the RADIUS server should assign an address. However, the RADIUS server is configured to receive a password. Because the client does not send a password, the RADIUS server does not send a framed prefix.

Note Ordinarily, the **ipv6 dhcp framed password** command will not need to be used because a client will have been authenticated as part of PPP session establishment.

Examples

The following example shows how to configure a password to be used with the RADIUS server:

```
Router(config-if)# ipv6 dhcp framed password password1
```

ipv6 dhcp guard attach-policy

To attach a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy, use the **ipv6 dhcp guard attach-policy** command in interface configuration or VLAN configuration mode. To unattach the DHCPv6 guard policy, use the **no** form of this command.

Syntax Available In Interface Configuration Mode

ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [... *vlan-id*]]

no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [... *vlan-id*]]

Syntax Available In VLAN Configuration Mode

ipv6 dhcp guard attach-policy [*policy-name*]

no ipv6 dhcp guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.
vlan	(Optional) Specifies that the DHCPv6 policy is to be attached to a VLAN.
add	(Optional) Attaches a DHCPv6 guard policy to the specified VLAN(s).
all	(Optional) Attaches a DHCPv6 guard policy to all VLANs.
except	(Optional) Attaches a DHCPv6 guard policy to all VLANs except the specified VLAN(s).
none	(Optional) Attaches a DHCPv6 guard policy to none of the specified VLAN(s).
remove	(Optional) Removes a DHCPv6 guard policy from the specified VLAN(s).
vlan-id	(Optional) Identity of the VLAN(s) to which the DHCP guard policy applies.

Command Default

No DHCPv6 guard policy is attached.

Command Modes

Interface configuration (config-if)

VLAN configuration (config-vlan)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to attach a DHCPv6 policy to an interface or to one or more VLANs. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to attach a DHCPv6 guard policy to an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp guard policy

To define a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy name, use the **ipv6 dhcp guard policy** command in global configuration mode. To remove the DHCPv6 guard policy name, use the **no** form of this command.

ipv6 dhcp guard policy [*policy-name*]
no ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Default

No DHCPv6 guard policy name is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command allows you to enter DHCPv6 guard configuration mode. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to define a DHCPv6 guard policy name:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

Related Commands

Command	Description
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*
ipv6 dhcp ping packets

Syntax Description

number	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.

Command Default

No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation

Examples

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note

The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

ipv6 dhcp relay destination *ipv6-address* [{*interface-type interface-number* | **vrf** *vrf-name* | **global**}]
no ipv6 dhcp relay destination *ipv6-address* [{*interface-type interface-number* | **vrf** *vrf-name* | **global**}]

Cisco CMTS Routers

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address***source-address*]
no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address** *source-address*]

Syntax Description

ipv6-address	Relay destination address. There are two types of relay destination address: • Link-scoped unicast or multicast IPv6 address. A user must specify an output interface for this kind of address. • Global or site-scoped unicast or multicast IPv6 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-number	(Optional) Interface type and number that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) associated with the relay destination IPv6 address.
global	(Optional) Specifies the relay destination when the relay destination is in the global address space and when the relay source is in a VRF.
link-address *link-address*	(Optional) Specifies the DHCPv6 link address. The link-address must be an IPv6 globally scoped address configured on the network interface where the DHCPv6 relay is operational.
source-address *source-address*	(Optional) Specifies the Cisco CMTS network interface source address. The source-address can be any IPv6 global-scoped address on the router.

Command Default

The relay function is disabled, and there is no relay destination on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added. The **global** keyword was added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
12.2(33)SCE5	This command was integrated into Cisco IOS Release 12.2(33)SCE5. The **link-address** and **source-address** keywords were added.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface
- A global or site-scoped unicast or multicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The **no** form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

In Cisco CMTS, if you change one or more parameters of this command, you have to disable the command using the no form, and execute the command again with changed parameters.

The default behavior (when **no source-address**, **link-address**, and **no output interface** commands are provisioned in the **ipv6 dhcp relay destination** command) of the new functionality is to copy the Cisco IOS SAS-computed source address to the link-address of the DHCPv6 relay-forward message.

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

The following example shows how to set the relay destination address on the Ethernet interface 4/3 on a Cisco CMTS router:

```
ipv6 dhcp relay destination 2001:db8:1234:5678:9abc:def1:2345:6789 ethernet 4/3
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the ipv6 dhcp-relay option vpn command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp-relay option vpn** command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the router. If the **ipv6 dhcp relay option vpn** command is enabled on a specified interface, it overrides the global **ipv6 dhcp-relay option vpn** command.

Examples

The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

ipv6 dhcp relay source-interface

To configure an interface to use as the source when relaying messages received on this interface, use the **ipv6 dhcp relay source-interface**command in interface configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp relay source-interface *type number*
no ipv6 dhcp relay source-interface *type number*

Syntax Description

type number	Interface type and number that specifies output interface for a destination. If these arguments are configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config-if)# ipv6 dhcp relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp-relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp-relay bulk-lease

To configure bulk lease query parameters, use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode. To remove the bulk-lease query configuration, use the **no** form of this command.

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds* | **retry** *number*} [**disable**]
no ipv6 dhcp-relay bulk-lease [**disable**]

Syntax Description

data-timeout	(Optional) Bulk lease query data transfer timeout.
seconds	(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.
retry	(Optional) Sets the bulk lease query retries.
number	(Optional) The range is from 0 to 5. The default is 5.
disable	(Optional) Disables the DHCPv6 bulk lease query feature.

Command Default

Bulk lease query is enabled automatically when the DHCP for IPv6 (DHCPv6) relay agent feature is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode to configure bulk lease query parameters, such as data transfer timeout and bulk-lease TCP connection retries.

The DHCPv6 bulk lease query feature is enabled automatically when the DHCPv6 relay agent is enabled. The DHCPv6 bulk lease query feature itself cannot be enabled using this command. To disable this feature, use the **ipv6 dhcp-relay bulk-lease**command with the **disable** keyword.

Examples

The following example shows how to set the bulk lease query data transfer timeout to 60 seconds:

```
Router(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

Related Commands

Command	Description

ipv6 dhcp-relay show bindings

To enable the DHCPv6 relay agent to list prefix delegation (PD) bindings, use the **ipv6 dhcp-relay show bindings**command in global configuration mode. To disable PD binding tracking, use the no form of this command.

ipv6 dhcp-relay show bindings
no ipv6 dhcp-relay show bindings

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **ipv6 dhcp-relay show bindings** command lists the PD bindings that the relay agent is tracking. The command lists the bindings in the relay's radix tree, lists DHCPv6 relay routes, and prints each entry's prefix and length, client identity association identification (IAID), and lifetime. <<Any more information here?>>

Examples

The following example enables the DHCPv6 relay agent to list PD bindings: <<OK?>>:

```
Router# ipv6 dhcp-relay show bindings
```

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface**command in global configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

interface-type interface-number	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [{*poolname* | **automatic**}] [**rapid-commit**] [**preference** *value*] [**allow-hint**]
no ipv6 dhcp server

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference *value*	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The **automatic** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable**command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCPv6 server VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on the router.

Examples

The following example enables the DHCPv6 server VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp server option vpn
```

ipv6 eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on a specified interface, use the **ipv6 eigrp** command in interface configuration mode. To disable EIGRP for IPv6, use the **no** form of this command.

ipv6 eigrp *as-number*
no ipv6 eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP is not enabled on an IPv6 interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **ipv6 eigrp** command to enable EIGRP for IPv6 on a per-interface basis.

If an autonomous system is specified, EIGRP for IPv6 is enabled only for the specified autonomous system. Otherwise, EIGRP for IPv6 is specified throughout the interface.

Examples

The following example enables EIGRP for IPv6 for AS 1 on Ethernet interface 0:

```
Router(config)# interface ethernet0
Router(config-if)# ipv6 eigrp 1
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.

ipv6 enable

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

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 general-prefix

To define an IPv6 general prefix, use the **ipv6 general-prefix** command in global configuration mode. To remove the IPv6 general prefix, use the **no** form of this command.

ipv6 general-prefix *prefix-name* {*ipv6-prefix/prefix-length* | **6to4** *interface-type interface-number* | **6rd** *interface-type interface-number*}
no ipv6 general-prefix *prefix-name*

Syntax Description

prefix-name	The name assigned to the prefix.
ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. When defining a general prefix manually, specify both the *ipv6-prefix* and **/** *prefix-length* arguments.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. When defining a general prefix manually, specify both the *ipv6-prefix* and **/** *prefix-length* arguments.
6to4	Allows configuration of a general prefix based on an interface used for 6to4 tunneling. When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number*argument.
interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function. When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number*argument.
6rd	Allows configuration of a general prefix computed from an interface used for IPv6 rapid deployment (6RD) tunneling.

Command Default

No general prefix is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	The optional **6rd** keyword was added.

Usage Guidelines

Use the ipv6 general-prefix command to define an IPv6 general prefix.

A general prefix holds a short prefix, based on which a number of longer, more specific, prefixes can be defined. When the general prefix is changed, all of the more specific prefixes based on it will change, too. This function greatly simplifies network renumbering and allows for automated prefix definition.

More specific prefixes, based on a general prefix, can be used when configuring IPv6 on an interface.

When defining a general prefix based on an interface used for 6to4 tunneling, the general prefix will be of the form 2002:a.b.c.d::/48, where "a.b.c.d" is the IPv4 address of the interface referenced.

Examples

The following example manually defines an IPv6 general prefix named my-prefix:

```
Router(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

The following example defines an IPv6 general prefix named my-prefix based on a 6to4 interface:

```
Router(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands

Command	Description
show ipv6 general-prefix	Displays information on general prefixes for an IPv6 addresses.

IPv6 Commands: ipv6 h to ipv6 mi

ipv6 hello-interval eigrp

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by an autonomous system number, use the **ipv6 hello-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hello-interval eigrp *as-number seconds*
no ipv6 hello-interval eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hello interval is 60 seconds. For all other networks, the default hello interval is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of EIGRP for IPv6, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds on autonomous system 1:

```
interface ethernet 0
 ipv6 hello-interval eigrp 1 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hold-time eigrp	Configures the hold time for a particular EIGRP for IPv6 routing process designated by the autonomous system number.

ipv6 hold-time eigrp

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by the autonomous system number, use the **ipv6 hold-time eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hold-time eigrp *as-number seconds*
no ipv6 hold-time eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hold-time interval is 180 seconds. For all other networks, the default hold-time interval is 15 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

Cisco recommends that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds for AS 1:

```
interface ethernet 0
 ipv6 hold-time eigrp 1 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

Command	Description
ipv6 hello-interval eigrp	Configures the hello interval for the EIGRP for IPv6 routing process designated by an autonomous system number.

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 *value*
no ipv6 hop-limit *value*

Syntax Description

value	The maximum number of hops. The acceptable range is from 1 to 255.

Command Default

The default is 64 hops.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example configures a maximum number of 15 hops for router advertisements and all IPv6 packets that are originated from the router:

```
Router(config)# ipv6 hop-limit 15
```

ipv6 host

To define a static host name-to-address mapping in the host name cache, use the **ipv6 host**command in global configuration mode. To remove the host name-to-address mapping, use the no form of this command.

ipv6 host *name* [*port*] *ipv6-address*
no ipv6 host *name*

Syntax Description

name	Name of the IPv6 host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
port	(Optional) The default Telnet port number for the associated IPv6 addresses.
ipv6-address	Associated IPv6 address. You can bind up to four addresses to a host name.

Command Default

Static host name-to-address mapping in the host name cache is not defined. The default Telnet port is 23.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The first character of the *name* variable can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
Device(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Device(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

Related Commands

Command	Description
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages, 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	The time interval between tokens being placed in the bucket. The acceptable range is from 0 to 2147483647 with a default of 100 milliseconds.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 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. The time interval between tokens placed in the bucket is 100 milliseconds. The maximum number of tokens stored in the bucket is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	Support for IPv6 ICMP rate limiting was extended to use token buckets.
12.0(21)ST	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command, with the support for IPv6 ICMP rate limiting extended to use token buckets, was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Release	Modification
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 icmp error-interval** command to limit the rate at which IPv6 ICMP error messages are sent. 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 arriving in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* 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** command to display IPv6 ICMP rate-limited counters.

Examples

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

```
ipv6 icmp error-interval 50 20
```

Related Commands

Command	Description
show ipv6 traffic	Displays statistics about IPv6 traffic.

ipv6 inspect

To apply a set of inspection rules to an interface, use the **ipv6 inspect** command in interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

ipv6 inspect *inspection-name* {**in** | **out**}
no ipv6 inspect *inspection-name* {**in** | **out**}

Syntax Description

inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

Command Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by Context-Based Access Control (CBAC).

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an inbound packet.

Examples

The following example applies a set of inspection rules named "outboundrules" to an external interface's outbound traffic. This causes inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
 ipv6 inspect outboundrules out
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of inspection rules.

ipv6 inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the ipv6 inspect alert off command in global configuration mode. To enable Cisco IOS firewall alert messages, use the no form of this command.

ipv6 inspect alert-off
no ipv6 inspect alert-off

Syntax Description

This command has no arguments or keywords.

Command Default

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example turns off CBAC alert messages:

```
ipv6 inspect alert-off
```

Related Commands

Command	Description
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each Cisco IOS firewall session closes, use the ipv6 inspect audit trail command in global configuration mode. To turn off Cisco IOS firewall audit trail message, use the no form of this command.

ipv6 inspect audit trail
no ipv6 inspect audit trail

Syntax Description

This command has no arguments or keywords.

Command Default

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ipv6 inspect audit trail
```

Afterward, audit trail messages such as the following are displayed:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes -- responder
 (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder
 (192.168.129.11:21) sent 325 bytes
```

These messages are examples of audit trail messages. To determine which protocol was inspected, refer to the responder's port number. The port number follows the responder's IP address.

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the ipv6 inspect max-incomplete high command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the no form of this command.

ipv6 inspect max-incomplete high *number*
no ipv6 inspect max-incomplete high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions. The value range is 1 through 4294967295.

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.

Command	Description
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ipv6 inspect max-incomplete low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ipv6 inspect max-incomplete low *number*
no ipv6 inspect max-incomplete low

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.

Command	Description
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect name

To define a set of ipv6 inspection rules, use the **ipv6 inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

ipv6 inspect name *inspection-name* *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
no ipv6 inspect name inspection-name [**protocol**]

Syntax Description

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.
protocol	A specified protocol. Possible protocol values are **icmp**, **udp**, **tcp**, and **ftp**. This value is optional in the **no** version of this command.
alert {**on** | **off**}	(Optional) For each inspected protocol, the generation of alert messages can be set be on or off. If no option is selected, alerts are generated based on the setting of the ipv6 inspect alert-off command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, the audit trail can be set on or off. If no option is selected, audit trail messages are generated based on the setting of the **ipv6 inspect audit-trail** command.
timeout *seconds*	(Optional) Specifies the number of seconds for a different idle timeout to override the global TCP or User Datagram Protocol (UDP) idle timeouts for the specified protocol. This timeout overrides the global TCP and UPD timeouts but will not override the global Domain Name System (DNS) timeout.
timeout seconds (fragmentation)	Configures the number of seconds that a packet state structure remains active. When the **timeout** value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default **timeout** value is 1 second. If this number is set to a value greater than 1 second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

Command Default

No set of inspection rules is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	FTP protocol support was added.

Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character limit. Define either one or two sets of rules per interface--you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or Internet Control Message Protocol (ICMP) as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol. To remove the entire set of named inspection rules, use the **no** form of this command with the specified inspection name.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (destination unreachable, echo-reply, time-exceeded, and packet too big) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

FTP Inspection

Cisco IOS Firewall uses layer 7 support for application modules such as FTP.

Cisco IOS IPv6 Firewall uses RFC 2428 to garner IPv6 addresses and corresponding ports. If an address other than an IPv6 address is present, the FTP data channel is not opened.

IPv6-specific port-to-application mapping (PAM) provides FTP inspection. PAM translates TCP or UDP port numbers into specific network services or applications. By mapping port numbers to network services or applications, an administrator can force firewall inspection on custom configurations not defined by well-known ports. PAM delivers with the standard well-known ports defined as defaults.

The table below describes the transport-layer and network-layer protocols.

Table 4: Protocol Keywords--Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	**icmp**
TCP	**tcp**
UDP	**udp**
FTP	**ftp**

Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ipv6 inspect name myrules tcp
ipv6 inspect name myrules udp audit-trail on
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ipv6 inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ipv6 inspect one-minute high**command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ipv6 inspect one-minute high *number*
no ipv6 inspect one-minute high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions . The default is 500 half-open sessions. Value range is 1 through 4294967295

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially-decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ipv6 inspect one-minute low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ipv6 inspect one-minute low *number*
no ipv6 inspect one-minute low

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect routing-header

To specify whether Context-based Access Control (CBAC) should inspect packets containing an IPv6 routing header, use the **ipv6 inspect routing-header** command. To drop packets containing an IPv6 routing header, use the no form of this command.

ipv6 inspect routing-header
no ipv6 inspect routing-header

Syntax Description

This command has no arguments or keywords.

Command Default

Packets containing IPv6 routing header are dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An IPv6 source uses the routing header to list one or more intermediate nodes to be visited between the source and destination of the packet. The Cisco IOS firewall uses this header to retrieve the destination host address. Cisco IOS firewall will establish the appropriate inspection session based on the retrieved address from the routing header.

The originating node lists all intermediate nodes that the packet must traverse. The source and destination address pair in the IPv6 header identifies the hop between the originating node and the first intermediate node. Once the first intermediate node receives the packet, it looks for a routing header. If the routing header is present, the next intermediate node address is swapped with the destination address in the IPv6 header and the packet is forwarded to the next intermediate node. This sequence continues for each intermediate node listed in the routing until no more entries exist in the routing header. The last entry in the routing header is the final destination address.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ip inspect routing-header
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect tcp finwait-time

To define how long a TCP session will be managed after the firewall detects a finish (FIN)-exchange, use the **ipv6 inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ipv6 inspect tcp finwait-time *seconds*
no ipv6 inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds. Valid values are from 1 to 2147483. If the FIN-exchange completes within the configured finwait time, the connection is closed normally.

Command Default

The default is 5 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-Based Access Control (CBAC) inspection is configured for the protocol of the packet, the software establishes state information for the new session.

Use this command to define how long a TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close. In a TCP connection, the client and the server terminate their end of the connection by sending a FIN message. The time that the client and the server wait for their FIN message to be acknowledged by each other before closing the sequence during a TCP connection is called the finwait time. The timeout that you set for the finwait time is referred to as the finwait timeout.

The global value specified for the finwait timeout applies to all TCP sessions inspected by CBAC.

Examples

The following example shows how to change the finwait timeout to 10 seconds:

```
ipv6 inspect tcp finwait-time 5
```

The following example shows how to change the finwait timeout back to the default (5 seconds):

```
no ipv6 inspect tcp finwait-time
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of IPv6 inspection rules.

ipv6 inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ipv6 inspect tcp idle-time** command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

ipv6 inspect tcp idle-time *seconds*
no ipv6 inspect tcp idle-time

Syntax Description

seconds	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).

Command Default

The default is 3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ipv6 inspect name** (global configuration) command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ipv6 inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ipv6 inspect tcp idle-time
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of IPv6 inspection rules.

ipv6 inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the **ipv6 inspect tcp max-incomplete host**command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

ipv6 inspect tcp max-incomplete host *number* **block-time** *minutes*
no ipv6 inspect tcp max-incomplete host

Syntax Description

number	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions. Value range is 1 through 4294967295
block-time	Specifies blocking of connection initiation to a host. Value range is 0 through 35791.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.

Command Default

The default is 50 half-open sessions and 0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, "half-open" means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *minutes* timeout is 0 (the default):

The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections inspected by Context-based Access Control (CBAC).

Examples

The following example changes the **max-incomplete host** number to 40 half-open sessions, and changes the **block-time** timeout to 2 minutes (120 seconds):

```
ipv6 inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ipv6 inspect tcp max-incomplete host
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ipv6 inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ipv6 inspect tcp synwait-time**command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ipv6 inspect tcp synwait-time *seconds*
no ipv6 inspect tcp synwait-time

Syntax Description

seconds	Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session . The default is 30 seconds. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the session's first SYN bit is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

Examples

The following example changes the "synwait" timeout to 20 seconds:

```
ipv6 inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ipv6 inspect tcp synwait-time
```

Related Commands

Command	Description
ipv6 inspect udp idle-time	Specifies the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity).

ipv6 inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the **ipv6 inspect udp idle-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ipv6 inspect udp idle-time *seconds*
no ipv6 inspect udp idle-time

Syntax Description

seconds	Specifies the length of time a UDP "session" will still be managed while there is no activity . The default is 30 seconds. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ipv6 inspect name**command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ipv6 inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ipv6 inspect udp idle-time
```

ipv6 local policy route-map

To enable local policy-based routing (PBR) for IPv6 packets, use the **ipv6 local policy route-map** command in global configuration mode. To disable local policy-based routing for IPv6 packets, use the **no** form of this command.

ipv6 local policy route-map *route-map-name*
no ipv6 local policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to be used for local IPv6 PBR. The name must match a *route-map-name* value specified by the **route-map** command.

Command Default

IPv6 packets are not policy routed.

Command Modes

Global configuration (config#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Packets originating from a router are not normally policy routed. However, you can use the **ipv6 local policy route-map** command to policy route such packets. You might enable local PBR if you want packets originated at the router to take a route other than the obvious shortest path.

The **ipv6 local policy route-map** command identifies a route map to be used for local PBR. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which packets should be policy routed. The **set** commands specify set actions, which are particular policy routing actions to be performed if the criteria enforced by the **match** commands are met. The **no ipv6 local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples

In the following example, packets with a destination IPv6 address matching that allowed by access list pbr-src-90 are sent to the router at IPv6 address 2001:DB8::1:

```
ipv6 access-list src-90
 permit ipv6 host 2001::90 2001:1000::/64
route-map pbr-src-90 permit 10
 match ipv6 address src-90
 set ipv6 next-hop 2001:DB8::1
ipv6 local policy route-map pbr-src-90
```

Related Commands

Command	Description
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 local pool

To configure a local IPv6 prefix pool, use the ipv6 local pool configuration command with the prefix pool name. To disband the pool, use the **no** form of this command.

ipv6 local pool poolname prefix/prefix-length assigned-length [**shared**] [**cache-size** *size*]
no ipv6 local pool poolname

Syntax Description

poolname	User-defined name for the local prefix pool.
prefix	IPv6 prefix assigned to the pool. 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 assigned to the pool. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
assigned-length	Length of prefix, in bits, assigned to the user from the pool. The value of the *assigned-length* argument cannot be less than the value of the / *prefix-length* argument.
shared	(Optional) Indicates that the pool is a shared pool.
cache-size *size*	(Optional) Specifies the size of the cache.

Command Default

No pool is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

All pool names must be unique.

IPv6 prefix pools have a function similar to IPv4 address pools. Contrary to IPv4, a block of addresses (an address prefix) are assigned and not single addresses.

Prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, the pool must be removed and recreated. All prefixes already allocated will also be freed.

Examples

This example shows the creation of an IPv6 prefix pool:

```
Router (config)# ipv6 local pool pool1 2001:0DB8::/29 64
Router# show ipv6 local pool
Pool Prefix Free In use
pool1  2001:0DB8::/29  65516  20
```

Related Commands

Command	Description
debug ipv6 pool	Enables IPv6 pool debugging.
peer default ipv6 address pool	Specifies the pool from which client prefixes are assigned for PPP links.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 local pool	Displays information about any defined IPv6 address pools.

ipv6 mfib

To reenable IPv6 multicast forwarding on the router, use the **ipv6 mfib** command in global configuration mode. To disable IPv6 multicast forwarding on the router, use the **no** form of this command.

ipv6 mfib
no ipv6 mfib

Syntax Description

The command has no arguments or keywords.

Command Default

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, IPv6 multicast forwarding is enabled. Because IPv6 multicast forwarding is enabled by default, use the **no** form of the **ipv6 mfib**command to disable IPv6 multicast forwarding.

Examples

The following example disables multicast forwarding on the router:

```
no ipv6 mfib
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 mfib-cef

To enable Multicast Forwarding Information Base (MFIB) Cisco Express Forwarding-based (interrupt level) IPv6 multicast forwarding for outgoing packets on a specific interface, use the **ipv6 mfib-cef**command in interface configuration mode. To disable CEF-based IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib-cef
no ipv6 mfib-cef

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Cisco Express Forwarding-based (interrupt level) IPv6 multicast forwarding is enabled by default when you enable Cisco Express Forwarding-based IPv6 multicast routing.

Use the **show ipv6 mfib interface** command to display the multicast forwarding interface status.

Examples

This example shows how to enable Cisco Express Forwarding-based IPv6 multicast forwarding:

```
Router(config-if)# ipv6 mfib-cef
```

This example shows how to disable Cisco Express Forwarding-based IPv6 multicast forwarding:

```
Router(config-if)# no ipv6 mfib-cef
```

Related Commands

Command	Description
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib cef output

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib cef output**command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib cef output
no ipv6 mfib cef output

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib cef output**command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib cef output
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib interface	Displays IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib fast

Note Effective in Cisco IOS Release 12.3(4)T, the **ipv6 mfib fast**command is replaced by the **ipv6 mfib cef output**command. See the **ipv6 mfib cef output**command for more information.

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib fast**command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib fast
no ipv6 mfib fast

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(4)T	The command was replaced by the ipv6 mfib cef output command.
12.2(25)S	The command was replaced by the ipv6 mfib cef output command.
12.0(28)S	The command was replaced by the ipv6 mfib cef output command.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib fast** command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib fast
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib interface	Displays IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib forwarding

To enable IPv6 multicast forwarding of packets received from a specific interface on the router, use the **ipv6 mfib forwarding**command in interface configuration mode. To disable IPv6 multicast forwarding of packets received from a specific interface, use the **no** form of this command.

ipv6 mfib forwarding
no ipv6 mfib forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **no ipv6 mfib forwarding** command is used to disable multicast forwarding of packets received from a specified interface, although the specified interface on the router will still continue to receive multicast packets destined for applications on the router itself.

Because multicast forwarding is enabled automatically when IPv6 multicast routing is enabled, the **ipv6 mfib forwarding** command is used to reenable multicast forwarding of packets if it has been previously disabled.

Examples

The following example shows how to disable multicast forwarding of packets from Ethernet 1/1:

```
Router(config) interface Ethernet1/1
Router(config-if) no ipv6 mfib forwarding
```

Related Commands

Command	Description
ipv6 mfib	Reenables IPv6 multicast forwarding on the router.

ipv6 mfib hardware-switching

To configure Multicast Forwarding Information Base (MFIB) hardware switching for IPv6 multicast packets on a global basis, use the **ipv6 mfib hardware-switching** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 mfib hardware-switching [{**connected** | **issu-support** | **replication-mode ingress** | **shared-tree** | **uplink**}]
no ipv6 mfib hardware-switching [{**connected** | **issu-support** | **replication-mode ingress** | **shared-tree** | **uplink**}]

Syntax Description

connected	(Optional) Allows you to download the interface and mask entry, and installs subnet entries in the access control list (ACL)-ternary content addressable memory (TCAM).
issu-support	(Optional) Enables In-Service Software Upgrade (ISSU) support for IPv6 multicast.
replication-mode ingress	(Optional) Sets the hardware replication mode to ingress.
shared-tree	(Optional) Sets the hardware switching for IPv6 multicast packets.
uplink	(Optional) Enables IPv6 multicast on the uplink ports of the Supervisor Engine 720-10GE.

Command Default

This command is enabled with the **connected** and **replication-mode ingress** keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXH	This command was modified. The **shared-tree** and the **uplink** keywords were added.
12.2(33)SXI	This command was modified. The **issu-support**keyword was added on the Supervisor Engine 4.
12.2(33)SXI2	This command was modified. The **issu-support**keyword was added on the Supervisor Engine 720 in distributed Cisco Express Forwarding (dCEF)-only mode.

Usage Guidelines

You must enter the **ipv6 mfib hardware-switching uplink** command to enable IPv6 multicast hardware switching on the standby Supervisor Engine 720-10GE.

Note The system message "PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL" is displayed on the Supervisor Engine if both the **fabric switching-mode allow dcef-only** and **ipv6 mfib hardware-switching uplink** commands are configured. The router will ignore the command configured last.

The **ipv6 mfib hardware-switching uplink** command ensures support of IPv6 multicast on standby uplink ports on systems that are configured with a Supervisor Engine 720-10GE only. You must reboot the system for this command to take effect. The MET space is halved on both the supervisor engines and the C+ modules.

Enabling the ipv6 mfib hardware-switching issu-support command will consume one Switched Port Analyzer (SPAN) session. This command will be effective if the image versions on the active and standby supervisors are different. If the command is not enabled, then the IPv6 multicast traffic ingressing and egressing from standby uplinks will be affected. This command is NVGENed. This command should be configured only once and preferably before performing the In-Service Software Upgrade (ISSU) load version process.

Note After completing the ISSU process, the administrator should disable the configured ipv6 mfib hardware-switching issu-support command.

Examples

The following example shows how to prevent the installation of the subnet entries on a global basis:

```
Router(config)# ipv6 mfib hardware-switching
```

The following example shows how to set the hardware replication mode to ingress:

```
Router(config)# ipv6 mfib hardware-switching replication-mode ingress
```

The following example shows how to enable IPv6 multicast on standby uplink ports on systems that are configured with a Supervisor Engine 720-10GE only:

```
Router(config)# ipv6 mfib hardware-switching uplink
Router(config)# end
Router# reload
```

Related Commands

Command	Description
f abric switching-mode allow dcef-only	Enables the truncated mode in the presence of two or more fabric-enabled switching modules.
show platform software ipv6-multicast	Displays information about the platform software for IPv6 multicast.

ipv6 mfib-mode centralized-only

To disable distributed forwarding on a distributed platform, use the **ipv6 mfib-mode centralized-only** command in global configuration mode. To reenable multicast forwarding, use the **no** form of this command.

ipv6 mfib-mode centralized-only
no ipv6 mfib-mode centralized-only

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast distributed forwarding is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Distributed forwarding is enabled by default when the **ipv6 multicast-routing**, **ipv6 cef distributed**, and the **ipv6 mfib** commands are enabled. The ipv6 mfib-mode centralized-only command disables distributed forwarding. All multicast forwarding is performed centrally.

Examples

The following example reenables distributed forwarding:

```
ipv6 mfib-mode centralized-only
```

ipv6 mld access-group

To perform IPv6 multicast receiver access control, use the **ipv6 mld access-group** command in interface configuration mode. To stop using multicast receiver access control, use the **no** form of this command.

ipv6 mld access-group *access-list-name*
no ipv6 mld access-group *access-list-name*

Syntax Description

access-list-name	A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

Command Default

All groups and sources are allowed.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The ipv6 mld access-group command is used for receiver access control and to check the groups and sources in Multicast Listener Discovery (MLD) reports against the access list. The **ipv6 mld access-group** command also limits the state created by MLD reports. Because Cisco supports MLD version 2, the **ipv6 mld access-group** command allows users to limit the list of groups a receiver can join. You can also use this command to allow or deny sources used to join Source Specific Multicast (SSM) channels.

If a report (S1, S2...Sn, G) is received, the group (0, G) is first checked against the access list. If the group is denied, the entire report is denied. If the report is allowed, each individual (Si, G) is checked against the access list. State is not created for the denied sources.

Examples

The following example creates an access list called acc-grp-1 and denies all the state for group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
```

```
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example creates an access list called acc-grp-1 and permits all the state for only group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example permits only EXCLUDE(G,{}) reports. This example converts EXCLUDE(G,{S1, S2..Sn}) into EXCLUDE(G,{}):

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 host :: host ff04::10
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example filters a particular source 100::1 for a group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 host 100::1 host ff04::10
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

ipv6 mld explicit-tracking

To enable explicit tracking of hosts, use the **ipv6 mld explicit-tracking**command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 mld explicit-tracking *access-list-name*
no ipv6 mld explicit-tracking *access-list-name*

Syntax Description

access-list-name	A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

Command Default

Explicit tracking is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When explicit tracking is enabled, the fast leave mechanism can be used with Multicast Listener Discovery (MLD) version 2 host reports. The *access-list-name* argument specifies a named IPv6 access list that can be used to specify the group ranges for which a user wants to apply explicit tracking.

Examples

The following example shows how to enable MLD explicit tracking on an access list named list1:

```
ipv6 mld explicit-tracking list1
```

ipv6 mld host-proxy

To enable the Multicast Listener Discovery (MLD) proxy feature, use the **ipv6 mld host-proxy** command in global configuration mode. To disable support for this feature, use the **no** form of this command.

ipv6 mld host-proxy [*group-acl*]
no ipv6 mld host-proxy

Syntax Description

group-acl	(Optional) Group access list (ACL).

Command Default

The MLD proxy feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mld host-proxy** command to enable the MLD proxy feature. If the *group-acl* argument is specified, the MLD proxy feature is supported for the multicast route entries that are permitted by the group ACL. If the *group-acl* argument is not provided, the MLD proxy feature is supported for all multicast routes present in multicast routing table.

Only one group ACL is configured at a time. Users can modify the group ACL by entering this command using a different *group-acl* argument.

Examples

The following example enables the MLD proxy feature for the multicast route entries permitted by the group ACL named "proxy-group":

```
Router(config)# ipv6 mld host-proxy proxy-group
```

Related Commands

Command	Description
ipv6 mld host-proxy interface	Enables the MLD proxy feature on a specified interface on an RP.
show ipv6 mld host-proxy	Displays IPv6 MLD host proxy information.

ipv6 mld host-proxy interface

To enable the Multicast Listener Discovery (MLD) proxy feature on a specified interface on a Route Processor (RP), use the **ipv6 mld host-proxy interface**command in global configuration mode. To disable the MLD proxy feature on a RP, use the **no** form of this command.

ipv6 mld host-proxy interface [*group-acl*]
no ipv6 mld host-proxy interface

Syntax Description

group-acl	(Optional) Group access list (ACL).

Command Default

The MLD proxy feature is not enabled on the RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mld host-proxy interface** command to enable the MLD proxy feature on a specified interface on an RP. If a router is acting as an RP for an multicast-route proxy entry, it generates an MLD report on the specified host-proxy interface. Only one interface can be configured as a host-proxy interface, and the host-proxy interface can be modified by using this command with a different interface name.

If a router is not acting as an RP, enabling this command does not have any effect, nor will it generate an error or warning message.

Examples

The following example specifies Ethernet 0/0 as the host-proxy interface:

```
Router (config)# ipv6 mld host-proxy interface Ethernet 0/0
```

Related Commands

Command	Description
ipv6 mld host-proxy	Enables the MLD proxy feature.
show ipv6 mld host-proxy	Displays IPv6 MLD host proxy information.

ipv6 mld join-group

To configure Multicast Listener Discovery (MLD) reporting for a specified group and source, use the **ipv6 mld join-group** command in interface configuration mode. To cancel reporting and leave the group, use the **no** form of this command.

ipv6 mld join-group [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** *acl* }

Syntax Description

group-address	(Optional) IPv6 address of the multicast group.
include	(Optional) Enables include mode.
exclude	(Optional) Enables exclude mode.
source-address	Unicast source address to include or exclude.
source-list	Source list on which MLD reporting is to be configured.
acl	(Optional) Access list used to include or exclude multiple sources for the same group.

Command Default

If a source is specified and no mode is specified, the default is to include the source.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **ipv6 mld join-group** command configures MLD reporting for a specified source and group. The packets that are addressed to a specified group address will be passed up to the client process in the device. The packets will be forwarded out the interface depending on the normal Protocol Independent Multicast (PIM) activity.

The **source-list** keyword and *acl* argument may be used to include or exclude multiple sources for the same group. Each source is included in the access list in the following format:

permit ipv6 host *source* **any**

If the **ipv6 mld join-group**command is repeated for the same group, only the most recent command will take effect. For example, if you enter the following commands, only the second command is saved and will appear in the MLD cache:

```
Device(config-if)# ipv6 mld join-group ff05::10 include 2000::1
Device(config-if)# ipv6 mld join-group ff05::10 include 2000::2
```

Examples

The following example configures MLD reporting for specific groups:

```
Device(config-if)# ipv6 mld join-group ff04::10
```

Related Commands

Command	Description
no ipv6 mld router	Disables MLD router-side processing on a specified interface.

ipv6 mld limit

To limit the number of Multicast Listener Discovery (MLD) states on a per-interface basis, use the **ipv6 mld limit** command in interface configuration mode. To disable a configured MLD state limit, use the **no** form of this command.

ipv6 mld limit *number* [**except** *access-list*]
no ipv6 mld limit *number* [**except** *access-list*]

Syntax Description

number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.
except	(Optional) Excludes an access list from the configured MLD state limit.
access-list	(Optional) Access list to exclude from the configured MLD state limit.

Command Default

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed per interface on a router when you configure this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was modified. It was integrated into Cisco IOS Release 12.2(50)SY.
15.0(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

Use the **ipv6 mld limit**command to configure a limit on the number of MLD states resulting from MLD membership reports on a per-interface basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache, and traffic for the excess membership reports is not forwarded.

Use the **ipv6 mld state-limit** command in global configuration mode to configure the global MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

If you do not configure the **except** *access-list* keyword and argument, all MLD states are counted toward the configured cache limit on an interface. Use the **except** *access-list* keyword and argument to exclude particular groups or channels from counting toward the MLD cache limit. An MLD membership report is counted against the per-interface limit if it is permitted by the extended access list specified by the **except***access-list* keyword and argument.

Examples

The following example shows how to limit the number of MLD membership reports on Ethernet interface 0:

```
interface ethernet 0
 ipv6 mld limit 100
```

The following example shows how to limit the number of MLD membership reports on Ethernet interface 0. In this example, any MLD membership reports from access list cisco1 do not count toward the configured state limit:

```
interface ethernet 0
 ipv6 mld limit 100 except cisco1
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the user to perform IPv6 multicast receiver access control.
ipv6 mld state-limit	Limits the number of MLD states on a global basis.

ipv6 mld query-interval

To configure the frequency at which the Cisco IOS software sends Multicast Listener Discovery (MLD) host-query messages, use the **ipv6 mld query-interval** command in interface configuration mode. To return to the default frequency, use the **no** form of this command.

ipv6 mld query-interval *seconds*
no ipv6 mld query-interval

Syntax Description

seconds	Frequency, in seconds, at which to send MLD host-query messages. It can be a number from 0 to 65535. The default is 125 seconds.

Command Default

The default is 125 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the router's attached networks. Hosts respond with MLD report messages indicating that they want to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group).

The designated router for a LAN is the only router that sends MLD host-query messages.

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command**should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-max-response-time** and **ipv6 mld query-timeout** commands. If you change the default value for the **ipv6 mld query-interval** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example sets the MLD query interval to 60 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-interval 60
```

Related Commands

Command	Description
ipv6 mld query-max- response-time	Configures the maximum response time advertised in MLD queries.
ipv6 mld query-timeout	Configures the timeout value before the router takes over as the querier for the interface.
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.
show ipv6 mld groups	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

ipv6 mld query-max-response-time

To configure the maximum response time advertised in Multicast Listener Discovery (MLD) queries, use the **ipv6 mld query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-max-response-time *seconds*
no ipv6 mld query-max-response-time

Syntax Description

seconds	Maximum response time, in seconds, advertised in MLD queries. The default value is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

Note If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command**should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval**and **ipv6 mld query-timeout** commands. If you change the default value for the **ipv6 mld query-max-response-time** command, make sure the changed value works correctly with these two commands.

> **Caution** Changing the default value may severely impact multicast forwarding.

Examples

The following example configures a maximum response time of 20 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-max-response-time 20
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 mld query-timeout	Configures the timeout value before the router takes over as the querier for the interface.
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.
show ipv6 mld groups	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

ipv6 mld query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the **ipv6 mld query-timeout**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-timeout *seconds*
no ipv6 mld query-timeout

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier.

Command Default

The default is 250 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command**should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval**and **ipv6 mld query-max-response-time**commands. If you change the default value for the **ipv6 mld query-timeout** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example configures the router to wait 130 seconds from the time it received the last query before it takes over as the querier for the interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-timeout 130
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 mld query-max- response-time	Configures the maximum response time advertised in MLD queries.

ipv6 mld router

To enable Multicast Listener Discovery (MLD) group membership message processing and routing on a specified interface, use the **ipv6 mld router**command in interface configuration mode. To disable MLD group membership message processing and routing on a specified interface, use the **no** form of the command.

ipv6 mld router
no ipv6 mld router

Syntax Description

This command has no arguments or keywords.

Command Default

MLD message processing and egress routing of multicast packets is enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

When the **ipv6 multicast-routing**commandis configured, MLD group membership message processing is enabled on every interface. The **no ipv6 mld router** command prevents forwarding (routing) of multicast packets to the specified interface and disables static multicast group configuration on the specified interface.

The **no ipv6 mld router** command also disables MLD group membership message processing on a specified interface. When MLD group membership message processing is disabled, the router stops sending MLD queries and stops keeping track of MLD members on the LAN.

If the **ipv6 mld join-group** command is also configured on an interface, it will continue with MLD host functionality and will report group membership when an MLD query is received.

MLD group membership processing is enabled by default. The **ipv6 multicast-routing**command does not enable or disable MLD group membership message processing.

Examples

The following example disables MLD group membership message processing on an interface and disables routing of multicast packets to that interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mld router
```

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

ipv6 mld snooping
no ipv6 mld snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping explicit-tracking

To enable explicit host tracking, use the **ipv6 mld snooping explicit-tracking** command in interface configuration mode. To disable explicit host tracking, use the **no** form of this command.

ipv6 mld snooping explicit-tracking
no ipv6 mld snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit host tracking is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Explicit host tracking is supported only with Internet Group Management Protocol Version 3 (IGMPv3) hosts.

When you enable explicit host tracking and the Cisco 7600 series router is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Cisco 7600 series router forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the Cisco 7600 series router does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Cisco 7600 series router works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that are reported by the host.
- The list of sources for each group that are reported by the hosts.

- The router filter mode of each group.
- The list of hosts for each group that request the source.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping explicit-tracking
```

Related Commands

Command	Description
ipv6 mld snooping limit	Configures the MLDv2 limits.
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping last-member-query-interval

To configure the last member query interval for Multicast Listener Discovery Version 2 (MLDv2) snooping, use the **ipv6 mld snooping last-member-query-interval** command in interface configuration. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping last-member-query-interval *interval*
no ipv6 mld snooping last-member-query-interval

Syntax Description

interval	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.

Command Default

The default is 1000 milliseconds (1 second).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Cisco 7600 series router waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no ipv6 mld snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes a higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ipv6 mld snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last member query interval to 200 milliseconds:

```
Router(config-if)#
ipv6 mld snooping last-member-query-interval 200
Router(config-if)#
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping limit

To configure Multicast Listener Discovery version 2 (MLDv2) protocol limits, use the **ipv6 mld snooping limit**command in global configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping limit {**l2-entry-limit** *max-entries* | **rate** *pps* | **track** *max-entries*}
no ipv6 mld snooping limit {**l2-entry-limit** | **rate** | **track**}

Syntax Description

l2-entry-limit *max-entries*	Specifies the maximum number of Layer 2 entries that can be installed by MLD snooping. Valid values are from 1 to 100000 entries.
rate *pps*	Specifies the rate limit of incoming MLDv2 messages. Valid values are from 100 to 6000 packets per second (pps).
track *max-entries*	Specifies the maximum number of entries in the explicit-tracking database. Valid values are from 0 to 128000 entries.

Command Default

The *max-entries*argument default is 32000 .

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 .

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* argument to 0, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries* value, a system logging message is generated.

When you reduce the *max-entries*argument, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to set the maximum number of Layer 2 entries that can be installed by MLD snooping:

```
Router(config)#
 ipv6 mld snooping limit l2-entry-limit 100000
```

This example shows how to set the rate limit for incoming MLDv2-snooping packets:

```
Router(config)#
 ipv6 mld snooping limit rate 200
```

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)#
 ipv6 mld snooping limit track 20000
```

This example shows how to disable software rate limiting:

```
Router(config)#
 no ipv6 mld snooping limit rate
```

Related Commands

Command	Description
ipv6 mld snooping explicit tracking	Enables explicit host tracking.

ipv6 mld snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ipv6 mld snooping mrouter** command in interface configuration mode.

ipv6 mld snooping mrouter interface *type slot/port*

Syntax Description

interface *type*	Specifies the interface type: valid values are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**
slot / *port*	Module and port number. The slash mark is required.

Command Default

No defaults are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure a Layer 2 port as a multicast router port:

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
```

Related Commands

Command	Description
mac-address-table static	Adds static entries to the MAC address table.
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping querier

To enable the Multicast Listener Discovery version 2 (MLDv2) snooping querier, use the **ipv6 mld snooping querier** command in interface configuration mode. To disable the MLDv2 snooping querier, use the **no** form of this command.

ipv6 mld snooping querier
no ipv6 mld snooping querier

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must configure an IPv6 address on the VLAN interface. When this feature is enabled, the MLDv2 snooping querier uses the IPv6 address as the query source address.

If there is no IPv6 address configured on the VLAN interface, the MLDv2 snooping querier does not start. The MLDv2 snooping querier disables itself if the IPv6 address is cleared. When this feature is enabled, the MLDv2 snooping querier restarts if you configure an IPv6 address.

The MLDv2 snooping querier:

- Does not start if it detects MLDv2 traffic from an IPv6 multicast router.
- Starts after 60 seconds if it detects no MLDv2 traffic from an IPv6 multicast router.
- Disables itself if it detects MLDv2 traffic from an IPv6 multicast router.

You can enable the MLDv2 snooping querier on all the Catalyst 6500 series switches in the VLAN that support it. One switch is elected as the querier.

Examples

This example shows how to enable the MLDv2 snooping querier on VLAN 200:

```
Router(config)# interface vlan 200
Router(config-if)# ipv6 mld snooping querier
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping report-suppression

To enable Multicast Listener Discovery version 2 (MLDv2) report suppression on a VLAN, use the **ipv6 mld snooping report-suppression** command in interface configuration mode. To disable report suppression on a VLAN, use the **no** form of this command.

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enable explicit tracking before enabling report suppression.

This command is supported on VLAN interfaces only.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping report-suppression
```

ipv6 mld ssm-map enable

To enable the Source Specific Multicast (SSM) mapping feature for groups in the configured SSM range, use the **ipv6 mld ssm-map enable**command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**
no ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **ipv6 mld ssm-map enable**command enables the SSM mapping feature for groups in the configured SSM range. When the **ipv6 mld ssm-map enable**command is used, SSM mapping defaults to use the Domain Name System (DNS).

SSM mapping is applied only to received Multicast Listener Discovery (MLD) version 1 or MLD version 2 membership reports.

Examples

The following example shows how to enable the SSM mapping feature:

```
Router(config)# ipv6 mld ssm-map enable
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.

Command	Description
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map query dns

To enable Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ipv6 mld ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map query dns**
no ipv6 mld [**vrf** *vrf-name*] **ssm-map query dns**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

DNS-based SSM mapping is enabled by default when the SSM mapping feature is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

DNS-based SSM mapping is enabled by default when the SSM mapping feature is enabled using the **ipv6 mld ssm-map enable** command. If DNS-based SSM mapping is disabled by entering the **no** version of the **ipv6 mld ssm-map query dns** command, only statically mapped SSM sources configured by the **ipv6 mld ssm-map static** command will be determined.

For DNS-based SSM mapping to succeed, the router needs to find at least one correctly configured DNS server.

Examples

The following example enables the DNS-based SSM mapping feature:

```
ipv6 mld ssm-map query dns
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.

Command	Description
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map static

To configure static Source Specific Multicast (SSM) mappings, use the **ipv6 mld ssm-map static**command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*
no ipv6 mld [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of the IPv6 access list that identifies a group range. Access list names cannot contain a space or quotation mark, or begin with a numeric.
source-address	Source address associated with an MLD membership for a group identified by the access list.

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **ipv6 mld ssm-map static** command to configure static SSM mappings. If SSM mapping is enabled and the router receives a Multicast Listener Discovery (MLD) membership for group G in the SSM range, the router tries to determine the source addresses associated with G by checking the **ipv6 mld ssm-map static** command configurations.

If group G is permitted by the access list identified by the *access-list* argument, then the specified source address is used. If multiple static SSM mappings have been configured using the **ipv6 mld ssm-map static** command and G is permitted by multiple access lists, then the source addresses of all matching access lists will be used (the limit is 20).

If no static SSM mappings in the specified access lists match the MLD membership, SSM mapping queries the Domain Name System (DNS) for address mapping.

Examples

The following example enables the SSM mapping feature and configures the groups identified in the access list named SSM_MAP_ACL_2 to use source addresses 2001:0DB8:1::1 and 2001:0DB8:1::3:

```
ipv6 mld ssm-map enable
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::1
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::3
ipv6 mld ssm-map query dns
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld state-limit

To limit the number of Multicast Listener Discovery (MLD) states globally, use the **ipv6 mld state-limit** command in global configuration mode. To disable a configured MLD state limit, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*
no ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.

Command Default

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed globally on a router when you configure this command.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was modified. It was integrated into Cisco IOS Release 12.2(50)SY.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ipv6 mld state-limit** command to configure a limit on the number of MLD states resulting from MLD membership reports on a global basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache and traffic for the excess membership reports is not forwarded.

Use the **ipv6 mld limit** command in interface configuration mode to configure the per-interface MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

Examples

The following example shows how to limit the number of MLD states on a router to 300:

```
ipv6 mld state-limit 300
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the performance of IPv6 multicast receiver access control.
ipv6 mld limit	Limits the number of MLD states resulting from MLD membership state on a per-interface basis.

ipv6 mld static-group

To statically forward traffic for the multicast group onto a specified interface and cause the interface to behave as if a Multicast Listener Discovery (MLD) joiner were present on the interface, use the **ipv6 mld static-group** command in interface configuration mode. To stop statically forwarding traffic for the specific multicast group, use the **no** form of this command.

ipv6 mld join-group [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** *acl* }

Syntax Description

group-address	(Optional) IPv6 address of the multicast group.
include	(Optional) Enables include mode.
exclude	(Optional) Enables exclude mode.
source-address	Unicast source address to include or exclude.
source-list	Source list on which MLD reporting is to be configured.
acl	(Optional) Access list used to include or exclude multiple sources for the same group.

Command Default

If no mode is specified for the source, use of the **include** keyword is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The ipv6 multicast-routing command must be configured for the **ipv6 mld static-group**command to be effective.

When the **ipv6 mld static-group** command is enabled, packets to the group are either fast-switched or hardware-switched, depending on the platform. Unlike what happens when using the **ipv6 mld join-group** command, a copy of the packet is not sent to the process level.

An access list can be specified to include or exclude multiple sources for the same group. Each source is included in the access list in the following format:

permit ipv6 host *source* **any**

Note Using the **ipv6 mld static-group** command is not sufficient to allow traffic to be forwarded onto the interface. Other conditions, such as the absence of a route, the router not being the designated router, or losing an assert, can cause the router not to forward traffic even if the **ipv6 mld static-group**command is configured.

Examples

The following example statically forward traffic for the multicast group onto the specified interface:

```
ipv6 mld static-group ff04::10 include 100::1
```

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
no ipv6 pim	Use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface.

IPv6 Commands: ipv6 mo to ipv6 ospf da

ipv6 mobile home-agent (global configuration)

To enter home agent configuration mode, use the **ipv6 mobile home-agent**command in global configuration mode. To reset to the default settings of the command, use the **no** form of this command.

ipv6 mobile home-agent
no ipv6 mobile home-agent

Syntax Description

This command has no arguments or keywords.

Command Default

Mobile IPv6 home agent is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mobile home-agent** command to enter home agent configuration mode. Once in home agent configuration mode, you can configure binding parameters using the **binding** command. Once an interface is configured to provide the home-agent service, the **ipv6 mobile home-agent**global configuration command automatically appears in the global configuration.

The home agent service needs to be started on each interface using the **ipv6 mobile home-agent**command in interface configuration mode. The **ipv6 mobile home-agent**command in global configuration mode does not start home agent service on an interface.

Examples

In the following example, the user enters home agent configuration mode:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)#
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

ipv6 mobile home-agent (interface configuration)

To initialize and start the Mobile IPv6 home agent on a specific interface, use the **ipv6 mobile home-agent**command in interface configuration mode. To discard bindings and any interface parameter settings, and to terminate home agent operation on a specific interface, use the **no** form of this command.

ipv6 mobile home-agent [**preference** *preference-value*]
no ipv6 mobile home-agent

Syntax Description

preference *preference-value*	(Optional) Configures the Mobile IPv6 home agent preference value on a specified interface. The *preference-value* argument is an integer to be configured for preference in the home agent information option. The range is from 0 to 65535. The default preference value is 0.

Command Default

Mobile IPv6 home agent is disabled. The default preference value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Before you enable the **ipv6 mobile home-agent** (interface configuration) command on an interface, you should configure common parameters using the **binding** command. Once an interface is configured to run the home agent feature, the **ipv6 mobile home-agent**command in global configuration mode automatically appears in the global configuration.

Once enabled, the **ipv6 mobile home-agent**(interface configuration) command cannot be disabled if there is a home agent configured on at least one of the interfaces. If there is no home agent service on any interfaces, the **no** form of the command disables home agent capability from the router.

To configure the home agent preference value, use the optional **preference** *preference-value* keyword and argument. A preference value is a 16-bit signed integer used by the home agent sending a router advertisement. The preference value orders the addresses returned to the mobile node in the home agent addresses field of a home agent address discovery reply message. The higher the preference value, the more preferable is the home agent.

If a preference value is not included in a router advertisement, the default value is 0. Values greater than 0 indicate a home agent more preferable than this default value.

Examples

In the following example, the user initializes and starts Mobile IPv6 agent on Ethernet interface 2:

```
Router(config)# interface Ethernet 2
Router(config-if)# ipv6 mobile home-agent
```

In the following example, the home agent preference value is set to 10:

```
Router(config-if)# ipv6 mobile home-agent preference 10
```

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

ipv6 mobile router

To enable IPv6 network mobility (NEMO) functionality on a router and place the router in IPv6 mobile router configuration mode, use the **ipv6 mobile router** command in global configuration mode. To disable NEMO functionality on the router, use the **no** form of the command.

ipv6 mobile router
no ipv6 mobile router

Syntax Description

This command has no arguments or keywords.

Command Default

NEMO functionality is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The mobile router is a router that operates as a mobile node. The mobile router can roam from its home network and still provide connectivity for devices on its networks. The mobile networks are locally attached to the router.

Examples

In the following example, the mobile router is enabled:

```
Router(config)# ipv6 mobile router
```

ipv6 mobile router-service roam

To enable the IPv6 mobile router interface to roam, use the **ipv6 mobile router-service roam** command in interface configuration mode. To disable roaming, use the **no** form of this command.

ipv6 mobile router-service roam [{**bandwidth-efficient** | **cost-efficient** | **priority** *value*}]
no ipv6 mobile router-service roam

Syntax Description

bandwidth-efficient	(Optional) Enables the mobile router to use the largest configured lifetime value.
cost-efficient	(Optional) Prevents a binding update unless a dialup link is up and a valid care-of address is available.
priority *value*	(Optional) Priority value that is compared among multiple configured interfaces to select the interface in which to send the registration request. When multiple interfaces have highest priority, the highest bandwidth is the preferred choice. When multiple interfaces have the same bandwidth, the interface with the highest IPv6 address is preferred. The range is from 0 to 255; the default is 100. Lower values equate to a higher priority.

Command Default

Roaming is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The mobile router discovers home agents and foreign agents by receiving agent advertisements.

The **bandwidth-efficient** keyword enables the mobile router to use the largest configured lifetime value, even when the home agent recommends a shorter lifetime in a binding refresh advice message. This option can be used when the bandwidth is expensive.

Examples

The following example shows how to enable roaming for the IPv6 mobile router interface:

```
Router(config-if)# ipv6 mobile router-service roam
```

Related Commands

Command	Description
show ipv6 mobile router	Displays configuration information and monitoring statistics about the IPv6 mobile router.

ipv6 mode host unicast

To disable IPv6 routing services and inhibit forwarding on an interface in the network, use the **ipv6 mode host unicast** command in interface configuration mode.

ipv6 mode host unicast
no ipv6 mode host unicast

Syntax Description

This command has no arguments or keywords

Command Default

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Prior to Cisco IOS 15.4(2)S	This command was introduced.
Cisco IOS 15.4(2)S	This command was deprecated.

Usage Guidelines

Ensure that the routing services on interfaces that forward IPv6 traffic is enabled.

Examples

The following example shows to configure how a specific route entries change when many parameters is monitored:

```
Device> enable
Device# configure terminal
Device(config)# interface Serial0/0
Device(config-if)# ipv6 mode host unicast
```

Related Commands

Command	Description

ipv6 mtu

To set the maximum transmission unit (MTU) size of IPv6 packets transmitted on an interface, use the **ipv6 mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*
no ipv6 mtu *bytes*

Syntax Description

bytes	MTU in bytes.

Command Default

The default MTU value depends on the interface medium, but the minimum for any interface is 1280 bytes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS 12.2(2)T	This command was introduced.
Cisco IOS 12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
Cisco IOS 12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
Cisco IOS 12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
Cisco IOS 12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS 12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS 12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS 12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE 3.10S	This command was modified. The range for *bytes* argument was extended to 9676 for loopback interfaces.

Usage Guidelines

If a nondefault value is configured for an interface, an MTU option is included in router advertisements.

IPv6 routers do not fragment forwarded IPv6 packets. Traffic originating from IPv6 routers may be fragmented.

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

In addition to the “IPv6 MTU value” (set by using the **ipv6 mtu** command), interfaces also have a nonprotocol-specific “MTU value”.

Note The MTU value configured by using the **ipv6 mtu** interface configuration command must not be less than 1280 bytes.

The MTU value configured depends on the type of interface. On a loopback interface, the MTU size can be a maximum of 9676 bytes.

Examples

The following example sets the maximum IPv6 packet size for serial interface 0/1 to 2000 bytes:

```
Device(config)# interface serial 0/1
Device(config-if)# ipv6 mtu 2000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 multicast aaa account receive

To enable authentication, authorization, and accounting (AAA) accounting on specified groups or channels, use the **ipv6 multicast aaa account receive**command in interface configuration mode. To disable AAA accounting, use the **no** form of this command.

ipv6 multicast aaa account receive *access-list-name* [**throttle** *throttle-number*]
no ipv6 multicast aaa account receive

Syntax Description

access-list-name	Access list to specify which groups or channels are to have AAA accounting enabled.
throttle	(Optional) Limits the number of records sent during channel surfing. No record is sent if a channel is viewed for less than a specified, configurable period of time.
throttle-number	(Optional) Throttle or surfing interval, in seconds.

Command Default

No AAA accounting is performed on any groups or channels.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Note Including information about IPv6 addresses in accounting and authorization records transmitted between the router and the RADIUS or TACACS+ server is supported. However, there is no support for using IPv6 to communicate with that server. The server must have an IPv4 address.

Use the **ipv6 multicast aaa account receive**command to enable AAA accounting on specific groups or channels and to set throttle interval limits on records sent during channel surfing.

Examples

The following example enables AAA accounting using an access list named list1:

```
Router(config-if)# ipv6 multicast aaa account receive list1
```

Related Commands

Command	Description
aaa accounting multicast default	Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.

ipv6 multicast boundary

To configure an IPv6 multicast boundary on the interface for a specified scope, use the **ipv6 multicast boundary** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 multicast boundary block source
no ipv6 multicast boundary block source
ipv6 multicast boundary scope *scope-value*
no ipv6 multicast boundary scope *scope-value*

Syntax Description

block source	Blocks the source of all incoming multicast traffic on an interface.
scope *scope-value*	Specifies the boundary for a particular scope. The scope value can be one of the following: • Link-local address • Subnet-local address • Admin-local address • Site-local address • Organization-local • Virtual Private Network (VPN) • Scope number, which is from 2 through 15

Command Default

Multicast boundary is not configured on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS 12.3(14)T	This command was introduced.
Cisco IOS 12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE 3.13S	This command was modified. The **block** and **source** keywords were added.

Usage Guidelines

Use the **ipv6 multicast boundary block source** command to block all incoming multicast traffic on an interface. However, this command allows the multicast traffic to flow out on the interface and allows any reserved multicast packets to flow in on the interface. This command is primarily used at first-hop routers to prevent local hosts from functioning as multicast sources.

If the **ipv6 multicast boundary scope** command is configured for a particular scope on the Reverse Path Forwarding (RPF) interface, then packets are not accepted on that interface for groups that belong to scopes that are less than or equal to the one that is configured. Protocol Independent Multicast (PIM) join/prune messages for those groups are not sent on the RPF interface. The effect of the scope is verified by checking the output of the **show ipv6 mrib route** command. The output does not show the RPF interface with Accept flag.

If the **ipv6 multicast boundary scope** command is configured for a particular scope on an interface in the outgoing interface list, packets are not forwarded for groups that belong to scopes that are less than or equal to the one configured.

Protocol Independent Multicast (PIM) join/prune (J/P) messages are not processed when it is received on the interface for groups that belong to scopes that are less than or equal to the one configured. Registers and bootstrap router (BSR) messages are also filtered on the boundary.

Examples

The following example shows how to block the source of all incoming multicast traffic on the interface:

```
Device> enable
Device# configure terminal
Device(config)# int GigabitEthernet0/0/0
Device(config-if)# ipv6 multicast boundary block source
```

The following example sets the scope value to be a scope number of 6:

```
ipv6 multicast boundary scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router to be a candidate BSR.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
show ipv6 mrib route	Displays the MRIB route information.

ipv6 multicast group-range

To disable multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router, use the **ipv6 multicast group-range**command in global configuration mode. To return to the command's default settings, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]
no ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list-name	(Optional) Name of an access list that contains authenticated subscriber groups and authorized channels that can send traffic to the router.

Command Default

Multicast is enabled for groups and channels permitted by a specified access list and disabled for groups and channels denied by a specified access list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 multicast group-range** command provides an access control mechanism for IPv6 multicast edge routing. The access list specified by the *access-list-name* argument specifies the multicast groups or channels that are to be permitted or denied. For denied groups or channels, the router ignores protocol traffic and actions (for example, no Multicast Listener Discovery (MLD) states are created, no mroute states are created, no Protocol Independent Multicast (PIM) joins are forwarded), and drops data traffic on all interfaces in the system, thus disabling multicast for denied groups or channels.

Using the **ipv6 multicast group-range** global configuration command is equivalent to configuring the MLD access control and multicast boundary commands on all interfaces in the system. However, the **ipv6 multicast group-range** command can be overridden on selected interfaces by using the following interface configuration commands:

- **ipv6 mld access-group** *access-list-name*
- **ipv6 multicast boundary scope** *scope-value*

Because the **no ipv6 multicast group-range** command returns the router to its default configuration, existing multicast deployments are not broken.

Examples

The following example ensures that the router disables multicast for groups or channels denied by an access list named list2:

```
Router(config)# ipv6 multicast group-range list2
```

The following example shows that the command in the previous example is overridden on an interface specified by int2:

```
Router(config)# interface int2
Router(config-if)# ipv6 mld access-group int-list2
```

On int2, MLD states are created for groups or channels permitted by int-list2 but are not created for groups or channels denied by int-list2. On all other interfaces, the access-list named list2 is used for access control.

In this example, list2 can be specified to deny all or most multicast groups or channels, and int-list2 can be specified to permit authorized groups or channels only for interface int2.

Related Commands

Command	Description
ipv6 mld access-group	Performs IPv6 multicast receiver access control.
ipv6 multicast boundary scope	Configures a multicast boundary on the interface for a specified scope.

ipv6 multicast limit

To configure per-interface multicast route (mroute) state limiters in IPv6, use the **ipv6 multicast limit** command in interface configuration mode. To remove the limit imposed by a per-interface mroute state limiter, use the **no** form of this command.

ipv6 multicast limit [{**connected** | **rpf** | **out**}] *limit-acl* *max* [**threshold** *threshold-value*]
no ipv6 multicast limit [{**connected** | **rpf** | **out**}] *limit-acl* *max* [**threshold** *threshold-value*]

Syntax Description

connected	(Optional) Limits mroute states created for an Access Control List (ACL)-classified set of multicast traffic on an incoming (Reverse Path Forwarding [RPF]) interface that is directly connected to a multicast source by counting each time that an mroute permitted by the ACL is created or deleted.
rpf	(Optional) Limits the number of mroute states created for an ACL-classified set of multicast traffic on an incoming (RPF) interface by counting each time an mroute permitted by the ACL is created or deleted.
out	(Optional) Limits mroute outgoing interface list membership on an outgoing interface for an ACL-classified set of multicast traffic by counting each time that an mroute list member permitted by the ACL is added or removed.
limit-acl	Name identifying the ACL that defines the set of multicast traffic to be applied to a per-interface mroute state limiter.
max	Maximum number of mroutes permitted by the per interface mroute state limiter. The range is from 0 to 2147483647.
threshold	(Optional) The mCAC threshold percentage.
threshold-value	(Optional) The specified percentage. The threshold notification default is 0%, meaning that threshold notification is disabled.

Command Default

No per-interface mroute state limiters are configured. Threshold notification is set to 0%; that is, it is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **ipv6 multicast limit** command to configure mroute state limiters on an interface.

For the required *limit-acl* argument, specify the ACL that defines the IPv6 multicast traffic to be limited on an interface. A standard or extended ACL can be specified.

The **ipv6 multicast limit cost**command complements the per-interface **ipv6 multicast limit**command. Once the *limit-acl* argument is matched in the **ipv6 multicast limit**command, the *access-list* argument in the **ipv6**

multicast limit costcommand is checked to see which cost to apply to limited groups. If no cost match is found, the default cost is 1.

The threshold notification for mCAC limit feature notifies the user when actual simultaneous multicast channel numbers exceeds or fall below a specified threshold percentage.

Examples

The following example configures the interface limit on the source router's outgoing interface Ethernet 1/3:

```
interface Ethernet1/3
ipv6 address FE80::40:1:3 link-local
 ipv6 address 2001:0DB8:1:1:3/64
 ipv6 multicast limit out acl1 10
```

Related Commands

Command	Description
ipv6 multicast limit cost	Applies a cost to mroutes that match per-interface mroute state limiters in IPv6.
ipv6 multicast limit rate	Configures the maximum allowed state on the source router.

ipv6 multicast limit cost

To apply a cost to mroutes that match per-interface mroute state limiters in IPv6, use t**he ipv6 multicast limit cost** command in global configuration mode. To restore the default cost for mroutes being limited by per-interface mroute state limiters, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*
no ipv6 multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Access Control List (ACL) name that defines the mroutes for which to apply a cost.
cost-multiplier	Cost value applied to mroutes that match the corresponding ACL. The range is from 0 to 2147483647.

Command Default

If the **ipv6 multicast limit cost** command is not configured or if an mroute that is being limited by a per-interface mroute state limiter does not match any of the ACLs applied to **ipv6 multicast limit cost**command configurations, a cost of 1 is applied to the mroutes being limited.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 multicast limit cost**command to apply a cost to mroutes that match per-interface mroute state limiters (configured with the **ipv6 multicast limit** command in interface configuration mode). This command is primarily used to provide bandwidth-based Call Admission Control (CAC) in network environments where multicast flows utilize different amounts of bandwidth. Accordingly, when this command is configured, the configuration is usually referred to as a bandwidth-based multicast CAC policy.

The **ipv6 multicast limit cost**command complements the per-interface **ipv6 multicast limit**command. Once the *limit-acl* argument is matched in the **ipv6 multicast limit**command, the *access-list* argument in the **ipv6 multicast limit cost**command is checked to see which cost to apply to limited groups. If no cost match is found, the default cost is 1.

Examples

The following example configures the global limit on the source router.

```
Router(config)# ipv6 multicast limit cost costlist1 2
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.

ipv6 multicast limit rate

To configure the maximum allowed state globally on the source router, use the **ipv6 multicast limit rate**command in global configuration mode. To remove the rate value, use the **no** form of this command.

ipv6 multicast limit rate *rate-value*
no ipv6 multicast limit rate *rate-value*

Syntax Description

rate-value	The maximum allowed state on the source router. The range is from 0 through 100.

Command Default

The maximum state is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The ipv6 multicast rate limit command is set to a maximum state of 1 message per second. If the default is set to 0, the syslog notification rate limiter is disabled.

Examples

The following example configures the maximum state on the source router:

```
ipv6 multicast limit rate 2
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.

ipv6 multicast multipath

To enable load splitting of IPv6 multicast traffic across multiple equal-cost paths, use the **ipv6 multicast multipath**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **multipath**
no ipv6 multicast [**vrf** *vrf-name*] **multipath**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 multicast multipath** command is enabled by default. In the default scenario, the reverse path forwarding (RPF) neighbor is selected randomly from the available equal-cost RPF neighbors, resulting in the load splitting of traffic from different sources among the available equal cost paths. All traffic from a single source is still received from a single neighbor.

When the **no ipv6 multicast multipath** command is configured, the RPF neighbor with the highest IPv6 address is chosen for all sources with the same prefix, even when there are other available equal-cost paths.

Because the **ipv6 multicast multipath**command changes the way an RPF neighbor is selected, it must be configured consistently on all routers in a redundant topology to avoid looping.

Examples

The following example enables load splitting of IPv6 traffic:

```
Router(config)# ipv6 multicast multipath
```

Related Commands

Command	Description
show ipv6 rpf	Checks RPF information for a given unicast host address and prefix.

ipv6 multicast pim-passive-enable

To enable the Protocol Independent Multicast (PIM) passive feature on an IPv6 router, use the **ipv6 multicast pim-passive-enable**command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 multicast pim-passive-enable
no ipv6 multicast pim-passive-enable

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **ipv6 multicast pim-passive-enable**command to configure IPv6 PIM passive mode on a router. Once PIM passive mode is configured globally, use the **ipv6 pim passive** command in interface configuration mode to configure PIM passive mode on a specific interface.

Examples

The following example configures IPv6 PIM passive mode on a router:

```
Router(config)# ipv6 multicast pim-passive-enable
```

Related Commands

Command	Description
ipv6 pim passive	Configures PIM passive mode on a specific interface.

ipv6 multicast-routing

To enable multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and to enable multicast forwarding, use the **ipv6 multicast-routing**command in global configuration mode. To stop multicast routing and forwarding, use the **no** form of this command.

ipv6 multicast-routing [**vrf** *vrf-name*]
no ipv6 multicast-routing

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Multicast routing is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **ipv6 multicast-routing**command to enable multicast forwarding. This command also enables Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router being configured.

You can configure individual interfaces before you enable multicast so that you can then explicitly disable PIM and MLD protocol processing on those interfaces, as needed. Use the **no ipv6 pim** or the **no ipv6 mld router** command to disable IPv6 PIM or MLD router-side processing, respectively.

For the Cisco Catalyst 6500 and Cisco 7600 series routers, you must enable the **ipv6 multicast-routing** command to use IPv6 multicast routing. The **ipv6 multicast-routing** command need not be enbaled for IPv6 unicast-routing to function.

Examples

The following example enables multicast routing and turns on PIM and MLD on all interfaces:

```
ipv6 multicast-routing
```

Related Commands

Command	Description
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
no ipv6 pim	Turns off IPv6 PIM on a specified interface.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.

ipv6 multicast rpf

To enable IPv6 multicast reverse path forwarding (RPF) check to use Border Gateway Protocol (BGP) unicast routes in the Routing Information Base (RIB), use the **ipv6 multicast rpf**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **rpf** {**backoff** *initial-delay max-delay* | **use-bgp**}
no ipv6 multicast [**vrf** *vrf-name*] **rpf** {**backoff** *initial-delay max-delay* | **use-bgp**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
backoff	Specifies the backoff delay after a unicast routing change.
initial-delay	Initial RPF backoff delay, in milliseconds (ms). The range is from 200 to 65535.
max-delay	Maximum RPF backoff delay, in ms. The range is from 200 to 65535.
use-bgp	Specifies to use BGP routes for multicast RPF lookups.

Command Default

The multicast RPF check does not use BGP unicast routes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI3	This command was integrated into Cisco IOS Release 12.2(33)SXI3.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **backoff** keyword and *initial-delay max-delay* arguments were added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When the **ipv6 multicast rpf** command is configured, multicast RPF check uses BGP unicast routes in the RIB. This is not done by default.

Examples

The following example shows how to enable the multicast RPF check function:

```
Router# configure terminal
Router(config)# ipv6 multicast rpf use-bgp
```

Related Commands

Command	Description
ipv6 multicast limit	Configure per-interface multicast route (mroute) state limiters in IPv6.
ipv6 multicast multipath	Enables load splitting of IPv6 multicast traffic across multiple equal-cost paths.

ipv6 nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation--Protocol Translation (NAT-PT), use the **ipv6 nat**command in interface configuration mode. To prevent the interface from being able to translate, use the **no** form of this command.

ipv6 nat
no ipv6 nat

Syntax Description

This command has no keywords or arguments.

Command Default

Traffic leaving or arriving at this interface is not subject to NAT-PT.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **ipv6 nat** command is usually specified on at least one IPv4 interface and one IPv6 interface at the networking device where you intend to use NAT-PT.

Examples

The following example assigns the IPv4 address 192.168.30.1 to Fast Ethernet interface 1/0 and the IPv6 address 2001:0DB8:0:1::1 to Fast Ethernet interface 2/0. IPv6 routing is globally enabled and both interfaces are configured to run IPv6 and enable NAT-PT translations.

```
interface fastethernet 1/0
 ip address 192.168.30.1 255.255.255.0
 ipv6 nat
!
interface fastethernet 2/0
 ipv6 address 2001:0DB8:0:1::1/64
 ipv6 nat
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address for an interface and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat max-entries

To specify the maximum number of Network Address Translation--Protocol Translation (NAT-PT) translation entries stored by the router, use the **ipv6 nat max-entries** command in global configuration mode. To restore the default number of NAT-PT entries, use the **no** form of this command.

ipv6 nat max-entries *number*
no ipv6 nat max-entries

Syntax Description

number	(Optional) Specifies the maximum number (1-2147483647) of NAT-PT translation entries. Default is unlimited.

Command Default

Unlimited number of NAT-PT entries.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Use the **ipv6 nat max-entries** command to set the maximum number of NAT-PT translation entries stored by the router when the router memory is limited, or the actual number of translations is important.

Examples

The following example sets the maximum number of NAT-PT translation entries to 1000:

```
ipv6 nat max-entries 1000
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat prefix

To assign an IPv6 prefix where matching IPv6 packets will be translated using Network Address Translation--Protocol Translation (NAT-PT), use the **ipv6 nat prefix**command in global configuration or interface configuration mode. To prevent the IPv6 prefix from being used by NAT-PT, use the **no** form of this command.

ipv6 nat prefix *ipv6-prefix/prefix-length*
no ipv6 nat prefix *ipv6-prefix/prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network used as the NAT-PT prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The only prefix length supported is 96. A slash mark must precede the decimal value.

Command Default

No IPv6 prefixes are used by NAT-PT.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **ipv6 nat prefix**command is used to specify an IPv6 address prefix against which the destination prefix in an IPv6 packet is matched. If the match is successful, NAT-PT will translate the IPv6 packet to an IPv4 packet using the configured mapping rules.

Use the **ipv6 nat prefix**command in global configuration mode to assign a global NAT-PTNAT-PT prefix, or in interface configuration mode to assign a different NAT-PT prefix for each interface. Using a different NAT-PT prefix on several interfaces allows the NAT-PT router to support an IPv6 network with multiple exit points to IPv4 networks.

Examples

The following example assigns the IPv6 prefix 2001:0DB8:1::/96 as the global NAT-PT prefix:

```
ipv6 nat prefix 2001:0DB8:1::/96
```

The following example assigns the IPv6 prefix 2001:0DB8:2::/96 as the NAT-PT prefix for the Fast Ethernet interface 1/0, and the IPv6 prefix 2001:0DB8:4::/96 as the NAT-PT prefix for the Fast Ethernet interface 2/0:

```
interface fastethernet 1/0
 ipv6 address 2001:0DB8:2:1::1/64
 ipv6 nat prefix 2001:0DB8:2::/96
!
```

```
interface fastethernet 2/0
 ipv6 address 2001:0DB8:4:1::1/64
 ipv6 nat prefix 2001:0DB8:4::/96
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address for an interface and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat prefix v4-mapped

To enable customers to send traffic from their IPv6 network to an IPv4 network without configuring IPv6 destination address mapping, use the **ipv6 nat prefix v4-mapped** command in global configuration or interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nat prefix *ipv6-prefix* **v4-mapped** {*access-list-nameipv6-prefix*}
no ipv6 nat prefix *ipv6-prefix* **v4-mapped** {*access-list-nameipv6-prefix*}

Syntax Description

ipv6-prefix	IPv6 prefix for Network Address Translation--Protocol Translation (NAT-PT).
access-list-name	Name of an IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

This command is not enabled.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The IPv6 target address of a packet arriving at an interface is checked to discover if it has a NAT-PT prefix that was configured with the **ipv6 nat prefix v4-mapped** command. If the prefix does match, then an access-list check is performed to discover if the source address matches the access list or prefix list. If the prefix does not match, the packet is dropped.

If the prefix matches, source address translation is performed. If a rule has been configured for the source address translation, the last 32 bits of the destination IPv6 address is used as the IPv4 destination and a flow entry is created.

Examples

In the following example, the access list permits any IPv6 source address with the prefix 2001::/96 to go to the destination with a 2000::/96 prefix. The destination is then translated to the last 32 bit of its IPv6 address; for example: source address = 2001::1, destination address = 2000::192.168.1.1. The destination then becomes 192.168.1.1 in the IPv4 network:

```
ipv6 nat prefix 2000::/96 v4-mapped v4map_acl
ipv6 access-list v4map_acl
 permit ipv6 2001::/96 2000::/96
```

ipv6 nat translation

To change the amount of time after which Network Address Translation--Protocol Translation (NAT-PT) translations time out, use the **ipv6 nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ipv6 nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout**} {*seconds* | **never**}
no ipv6 nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout**}

Syntax Description

timeout	Specifies that the timeout value applies to dynamic translations. Default is 86400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes).
dns-timeout	Specifies that the timeout value applies to connections to the Domain Naming System (DNS). Default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86400 seconds (24 hours).
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.
syn-timeout	Specifies that the timeout value applies when a TCP SYN (request to synchronize sequence numbers used when opening a connection) flag is received but the flag is not followed by data belonging to the same TCP session.
seconds	Number of seconds after which the specified translation timer expires. The default is 0.
never	Specifies that the dynamic translation timer never expires.

Command Default

timeout : 86400 seconds (24 hours)**udp-timeout**: 300 seconds (5 minutes)**dns-timeout**: 60 seconds (1 minute)**tcp-timeout**: 86400 seconds (24 hours)**finrst-timeout:**60 seconds (1 minute)**icmp-timeout**: 60 seconds (1 minute)

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Dynamic translations time out after a period of time without any translations. The default timeout period is 24 hours. When port translation is configured, there is finer control over translation entry timeouts because each entry contains more context about the traffic that is using it. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless an RST or FIN flag is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example causes UDP port translation entries to time out after 10 minutes:

```
ipv6 nat translation udp-timeout 600
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v4v6 pool

To define a pool of IPv6 addresses for Network Address Translation--Protocol Translation (NAT-PT), use the **ipv6 nat v4v6 pool**command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length*
no ipv6 nat v4v6 pool *name start-ipv6 end-ipv6* **prefix-length** *prefix-length*

Syntax Description

name	Name of the pool.
start-ipv6	Starting IPv6 address that defines the range of IPv6 addresses in the address pool.
end-ipv6	Ending IPv6 address that defines the range of IPv6 addresses in the address pool.
prefix-length *prefix-length*	Number that indicates how many bits of the address indicate the network. Specify the subnet of the network to which the pool addresses belong.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command defines a pool of IPv6 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of an IPv6 address to translate an IPv4 address.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2. One static NAT-PT mapping is configured to access a Domain Naming System (DNS) server. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address 2001:0DB8:AABB:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat v6v4 source 2001:0DB8:AABB:1::1 10.21.8.0
ipv6 nat prefix 2001:0DB8:EEFF::/96
```

```
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

Related Commands

Command	Description
clear ipv6 nat translations	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v4v6 source

To configure IPv4 to IPv6 address translation using Network Address Translation--Protocol Translation (NAT-PT), use the **ipv6 nat v4v6 source**command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

ipv6 nat v4v6 source {**list** {*access-list-numbername*} **pool** *name* | *ipv4-address ipv6-address*}
no ipv6 nat v4v6 source {**list** {*access-list-numbername*} **pool** *name* | *ipv4-address ipv6-address*}

Syntax Description

list *access-list-number*	Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *name*	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
ipv4-address	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
ipv6-address	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.

Command Default

No NAT-PT translation of IPv4 to IPv6 addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv4 addresses that match the standard access list are translated using IPv6 addresses allocated from the pool named with the **ipv6 nat v4v6 pool** command. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form using the *ipv4-address* and *ipv6-address*arguments establishes a single static translation.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address 2001:0DB8:AABB:1::9/64
 ipv6 enable
```

```
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat prefix 3ffe:c00:yyyy::/96
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

The following example shows a static translation where the IPv4 address 192.168.30.1 is translated into the IPv6 address 2001:0DB8:EEFF::2:

```
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.
ipv6 nat v4v6 pool	Defines a pool of IPv6 addresses for NAT-PT.
ipv6 nat v6v4 source	Enables NAT-PT for an IPv6 source address.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v6v4 pool

To define a pool of IPv4 addresses for Network Address Translation--Protocol Translation (NAT-PT), use the **ipv6 nat v6v4 pool**global configuration command. To remove one or more addresses from the pool, use the **no** form of this command.

ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length*
no ipv6 nat v6v4 pool *name start-ipv4 end-ipv4* **prefix-length** *prefix-length*

Syntax Description

name	Name of the pool.
start-ipv4	Starting IPv4 address that defines the range of IPv4 addresses in the address pool.
end-ipv4	Ending IPv4 address that defines the range of IPv4 addresses in the address pool.
prefix-length *prefix-length*	Number that indicates how many bits of the address indicate the network. Specify the subnet of the network to which the pool addresses belong.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This command defines a pool of IPv4 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of IPv4 addresses to translate IPv6 addresses.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1. One static NAT-PT mapping is configured to access a Domain Naming System (DNS) server. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address 2001:0DB8:AABB:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
ipv6 nat prefix 2001:0DB8:EEFF::/96
```

```
!
ipv6 access-list pt-list1
 permit ipv6 2001:0DB8:AABB:1::/64 any
```

Related Commands

Command	Description
clear ipv6 nat translations	Clears dynamic NAT-PT translations from the translation table.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nat v6v4 source

To configure IPv6 to IPv4 address translation using Network Address Translation--Protocol Translation (NAT-PT), use the **ipv6 nat v6v4 source**command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

ipv6 nat v6v4 source {**list** *access-list-name* **pool** *name* | **route-map** *map-name* **pool** *name* | *ipv6-address ipv4-address*} [**overload**]
no ipv6 nat v6v4 source {**list** *access-list-name* **pool** *name* | **route-map** *map-name* **pool** *name* | *ipv6-address ipv4-address*} [**overload**]

Syntax Description

list *access-list-name*	IPv6 access list name. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
route-map *map-name*	Sets up a single static translation. This keyword and argument combination establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
ipv6-address	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.
ipv4-address	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
overload	Enables multiplexing of IPv6 addresses to a single IPv4 address for TCP, UDP, and ICMD.

Command Default

No NAT-PT translation of IPv6 to IPv4 addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(2)T	The **overload** keyword was added to support Port Address Translation (PAT), or Overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool.

Usage Guidelines

Dynamic and Static Address Translation

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv6 addresses that match the IPv6 access list are translated using IPv4 addresses allocated from the pool named with the **ipv6 nat v6v4 pool** command. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form using the *ipv6-address* and *ipv4-address*arguments establishes a single static translation.

Port Address Translation

When used for PAT, the command can be used for a single IPv4 interface or for a pool of IPv4 interfaces.

Examples

Dynamic Mapping to a Pool of IPv4 Addresses Example

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
 ipv6 address ffe:aaaa:bbbb:1::9/64
 ipv6 enable
 ipv6 nat
!
interface Ethernet3/3
 ip address 192.168.30.9 255.255.255.0
 ipv6 nat
!
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
ipv6 nat prefix 3ffe:c00:::/96
!
ipv6 access-list pt-list1
 permit ipv6 3ffe:aaaa:bbbb:1::/64 any
```

Static Translation for a Single Address Example

The following example shows a static translation where the IPv6 address 3ffe:aaaa:bbbb:1::1 is translated into the IPv4 address 10.21.8.10:

```
ipv6 nat v6v4 source 3ffe:aaaa:bbbb:1::1 10.21.8.10
```

Port Address Translation to a Single Address Example

```
ipv6 nat v6v4 pool v6pool 10.1.1.1 10.1.1.10 subnetmask 255.255.255.0
ipv6 nat v6v4 source list v6list interface e1 overload
ipv6 accesslist v6list
permit 3000::/64 any
```

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.
debug ipv6 nat	Diaplays debugging messages for NAT-PT.
ipv6 nat v6v4 pool	Defines a pool of IPv4 addresses for NAT-PT.

Command	Description
ipv6 nat v4v6 source	Enables NAT-PT for an IPv4 source address.
show ipv6 nat translations	Displays active NAT-PT translations.

ipv6 nd advertisement-interval

To configure the advertisement interval option in router advertisements (RAs), use the **ipv6 nd advertisement-interval** in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

ipv6 nd advertisement-interval
no ipv6 nd advertisement-interval

Syntax Description

This command has no arguments or keywords.

Command Default

Advertisement interval option is not sent.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
15.2(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Use the **ipv6 nd advertisement-interval**command to indicate to a visiting mobile node the interval at which that node may expect to receive RAs. The node may use this information in its movement detection algorithm.

Examples

The following example enables the advertisement interval option to be sent in RAs:

```
Device(config-if)# ipv6 nd advertisement-interval
```

Related Commands

Command	Description
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
ipv6 nd ra-interval	Configures the interval between Mobile IPv6 RA transmissions on an interface.

ipv6 nd autoconfig default-router

To allow Neighbor Discovery to install a default route to the Neighbor Discovery-derived default router, use the **ipv6 nd autoconfig default-router** command in interface configuration mode. To remove the default route configured through interface configuration mode from the interface, use the **no** form of this command.

ipv6 nd autoconfig default-router
no ipv6 nd autoconfig default-router

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled in host mode.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

If the **ipv6 nd autoconfig default-router** command is configured on a router, Neighbor Discovery installs a default route to the Neighbor Discovery-derived default router. Using this command sends a router solicitation (RS) message to solicit a router advertisement (RA), thus eliminating any delay in waiting for the next periodic RA.

Examples

```
Device(config-if)# ipv6 nd autoconfig default router
```

Related Commands

Command	Description
ipv6 nd autoconfig prefix	Uses Neighbor Discovery to install all valid on-link prefixes from RAs received on the interface.
ipv6 nd route-owner	Inserts Neighbor Discovery-learned routes into the routing table with "ND" status and enables ND autoconfiguration behavior.

ipv6 nd autoconfig prefix

To use Neighbor Discovery to install all valid on-link prefixes from router advertisements (RAs) received on the interface, use the **ipv6 nd autoconfig prefix** command in interface configuration mode. To remove the prefix from the RIB, use the **no** form of the command.

ipv6 nd autoconfig prefix
no ipv6 nd autoconfig prefix

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Using the **ipv6 nd autoconfig prefix command** command sends a router solicitation (RS) message to solicit a router advertisement (RA), thus eliminating any delay in waiting for the next periodic RA. The router receives a prefix from a neighboring router, and installs the prefix in the RIB.

Use of the **ipv6 nd autoconfig prefix command** command allows Neighbor Discovery to install all valid on-link prefixes from RAs received on the interface. The prefixes are installed as Neighbor Discovery-owned static routes in same manner as a Neighbor Discovery default route. If both **ipv6 address autoconfig** and **ipv6 nd autoconfig prefix** are both configured, then the handling of /64 autoconfiguration and on-link prefixes will be unchanged. All other valid Neighbor Discovery prefixes will be installed as static routes.

Examples

```
Device(config-if)# ipv6 nd autoconfig default-router
```

Related Commands

Command	Description
ipv6 nd autoconfig default-router	Allows Neighbor Discovery to install a default route to the Neighbor Discovery-derived default router.
ipv6 nd route-owner	Inserts Neighbor Discovery-learned routes into the routing table with "ND" status and enables ND autoconfiguration behavior.

ipv6 nd cache expire

To configure the length of time before an IPv6 neighbor discovery (ND) cache entry expires, use the **ipv6 nd cache expire** command in interface configuration mode. To remove this configuration, use the **no** form of this command.

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

Syntax Description

expire-time-in-seconds	The time range is from 1 through 65536 seconds. The default is 14400 seconds, or 4 hours.
refresh	(Optional) Automatically refreshes the ND cache entry.

Command Default

This expiration time is 14400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

By default, an ND cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds, or 4 hours. The **ipv6 nd cache expire** command allows the user to vary the expiry time and to trigger autorefresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, an ND cache entry is autorefreshed. The entry moves into the DELAY state and the neighbor unreachability detection (NUD) process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation (NS) is sent and then retransmitted as per the configuration.

Examples

The following example shows that the ND cache entry is configured to expire in 7200 seconds, or 2 hours:

```
Router(config-if)# ipv6 nd cache expire 7200
```

ipv6 nd cache interface-limit (global)

To configure a neighbor discovery cache limit on all interfaces on the device, use the **ipv6 nd cache interface-limit**command in global configuration mode. To remove the neighbor discovery from all interfaces on the device, use the **no** form of this command.

ipv6 nd cache interface-limit *size* [**log** *rate*]
no ipv6 nd cache interface-limit *size* [**log** *rate*]

Syntax Description

size	Cache size.
log *rate*	(Optional) Adjustable logging rate, in seconds. The valid values are 0 and 1.

Command Default

Default logging rate for the device is one entry every second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **ipv6 nd cache interface-limit**command in global configuration mode imposes a common per-interface cache size limit on all interfaces on the device.

Issuing the **no** or default form of the command will remove the neighbor discovery limit from every interface on the device that was configured using global configuration mode. It will not remove the neighbor discovery limit from any interface configured using the **ipv6 nd cache interface-limit**command in interface configuration mode.

The default (and maximum) logging rate for the device is one entry every second.

Examples

The following example shows how to set a common per-interface cache size limit of 4 seconds on all interfaces on the device:

```
Device(config)#
 ipv6 nd cache interface-limit 4
```

Related Commands

Command	Description
ipv6 nd cache interface-limit (interface)	Configures a neighbor discovery cache limit on a specified interface on the device.

ipv6 nd cache interface-limit (interface)

To configure a neighbor discovery cache limit on a specified interface on the , use the **ipv6 nd cache interface-limit**command in interface configuration mode. To remove the neighbor discovery limit configured through interface configuration mode from the interface, use the **no** form of this command.

ipv6 nd cache interface-limit *size* [**log** *rate*]
no ipv6 nd cache interface-limit *size* [**log** *rate*]

Syntax Description

size	Cache size.
log *rate*	(Optional) Adjustable logging rate, in seconds. The valid values are 0 and 1.

Command Default

Default logging rate for the device is one entry every second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ipv6 nd cache interface-limit** command in interface configuration mode allows you to configure a per-interface neighbor discovery limit on the associated interface. The limit configured by this command overrides any limit configured using the **ipv6 nd cache interface-limit** command in global configuration mode.

Issuing the **no** or default form of the command removes the neighbor discovery limit configured using interface configuration mode from the interface. Then, if the **ipv6 nd cache interface-limit** command in global configuration mode has been issued, the neighbor discovery limit on the interface reverts to that specified by global configuration. If the globally configured limit is smaller than the interface limit, then excess entries are removed. If the **ipv6 nd cache interface-limit** command in global configuration mode has not been issued, then no limit is set on the interface.

The number of entries in the neighbor discovery cache is limited on an interface basis. Once the limit is reached, no new entries are allowed.

Examples

The following example shows how to set the number of entries in a neighbor discovery cache (on an interface basis) to 1:

```
Device(config-if)# ipv6 nd cache interface-limit 1
```

Related Commands

Command	Description
ipv6 nd cache interface-limit (global)	Configures a neighbor discovery cache limit on all interfaces on the devices.

ipv6 nd dad attempts

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

ipv6 nd dad attempts *value*
no ipv6 nd dad attempts *value*

Syntax Description

value	The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. Default is one message.

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SNG	Th is command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 2462, IPv6 Stateless Address Autoconfiguration) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on a tentative unicast IPv6 address.

The interval between 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 resolving the address or when probing the reachability of a neighbor. 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:

```
%IPV6-4-DUPLICATE: Duplicate address FE80::1 on Ethernet0
```

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 Ethernet0
```

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:

- ATM permanent virtual circuit (PVC)
- Cisco High-Level Data Link Control (HDLC)
- Ethernet, Fast Ethernet, and Gigabit Ethernet
- FDDI
- Frame Relay PVC
- Point-to-point links
- PPP

Examples

The following example configures five consecutive neighbor solicitation messages to be sent on Ethernet interface 0 while duplicate address detection is being performed on the tentative unicast IPv6 address of the interface. The example also disables duplicate address detection processing on Ethernet interface 1.

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 nd dad attempts 5
Device(config)# interface ethernet 1
Device(config-if)# ipv6 nd dad attempts 0
```

Note Configuring a value of 0 with the **ipv6 nd dad attempts** command disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. The default is one message.

To display the state (OK, TENTATIVE, or DUPLICATE) of the unicast IPv6 address configured for an interface, to verify whether duplicate address detection is enabled on the interface, and to verify the number of consecutive duplicate address detection, neighbor solicitation messages that are being sent on the interface, enter the **show ipv6 interface** command:

```
Device# show ipv6 interface
Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1 [TENTATIVE]
  Global unicast address(es):
    2000::1, subnet is 2000::/64 [TENTATIVE]
    3000::1, subnet is 3000::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised 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.
Ethernet1 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::2
  Global unicast address(es):
    2000::2, subnet is 2000::/64
    3000::3, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is disabled, number of DAD attempts: 0
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
```

```
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd dad-proxy

To enable the IPv6 Neighbor Discovery (ND) Duplicate Address Detection (DAD) Proxy feature, use the **ipv6 nd dad-proxy** command in global configuration mode or interface configuration mode.

ipv6 nd dad-proxy
noipv6 nd dad-proxy

Command Default

The IPv6 ND DAD Proxy feature is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)SG	This command was introduced.

Usage Guidelines

Use the **ipv6 nd dad-proxy** command to enable the IPv6 ND DAD Proxy feature on a device or an interface.

On devices where the IPv6 ND Multicast Suppress feature is not available on the device platform, you use the **ipv6 nd dad-proxy** command in global configuration mode to configure the feature on the device.

The following example shows how to configure IPv6 ND DAD proxy on a device:

```
Device(config)# ipv6 nd dad-proxy
```

ipv6 nd dad time

To configure the neighbor solicitation (NS) retransmit interval for duplicate address detection (DAD) separately from the NS retransmit interval for address resolution, use the **ipv6 nd dad time** command in global configuration or interface configuration mode. To remove the NS retransmit interval for DAD, use the **no** form of this command.

ipv6 nd dad time *milliseconds*
no ipv6 nd dad time

Syntax Description

milliseconds	The interval between IPv6 neighbor solicit transmissions for DAD. The range is from 1000 to 3600000 milliseconds.

Command Default

Default NS retransmit interval: 1000 msec (1 second)

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3S	This command was introduced.

Usage Guidelines

The **ipv6 nd dad time** command allows you to configure the NS retransmit interval for DAD separately from the NS retransmit interval for address resolution. This command also allows you to set the behavior globally for the whole router or on a per-interface basis.

Examples

The following example shows how to increase the default NS retransmit interval on an interface for address resolution to 3 seconds but keep the DAD NS retransmit interval at the default value of 1 second:

```
Router(config-if)# ipv6 nd ns-interval 3000
Router(config-if)# ipv6 nd dad time 1000
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions for address resolution on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd host mode strict

To enable the conformant, or strict, IPv6 host mode, use the **ipv6 nd host mode strict** command in global configuration mode. To reenable conformant, or loose, IPv6 host mode, use the **no** form of this command.

ipv6 nd host mode strict

Syntax Description

This command has no arguments or keywords.

Command Default

Nonconformant, or loose, IPv6 host mode is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

The default IPv6 host mode type is loose, or nonconformant. To enable IPv6 strict, or conformant, host mode, use the **ipv6 nd host mode strict** command. You can change between the two IPv6 host modes using the **no** form of this command.

The **ipv6 nd host mode strict** command selects the type of IPv6 host mode behavior and enters interface configuration mode. However, the **ipv6 nd host mode strict** command is ignored if you have configured IPv6 routing with the **ipv6 unicast-routing** command. In this situation, the default IPv6 host mode type, loose, is used.

Examples

The following example shows how to configure the device as a strict IPv6 host and enables IPv6 address autoconfiguration on Ethernet interface 0/0:

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address autoconfig
```

The following example shows how to configure the device as a strict IPv6 host and configures a static IPv6 address on Ethernet interface 0/0:

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address 2001::1/64
```

Related Commands

Command	Description
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.

ipv6 nd inspection

To apply the Neighbor Discovery Protocol (NDP) Inspection feature, use the **ipv6 nd inspection** command in interface configuration mode. To remove the NDP Inspection feature, use the **no** form of this command.

ipv6 nd inspection [**attach-policy** [*policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} **vlan** *vlan-id*]]
no ipv6 nd inspection

Syntax Description

attach-policy	(Optional) Attaches an NDP Inspection policy.
policy-name	(Optional) The NDP Inspection policy name.
vlan	(Optional) Applies the ND Inspection feature to a VLAN on the interface.
add	(Optional) Adds a VLAN to be inspected.
except	(Optional) Inspects all VLANs except the one specified.
none	(Optional) Specifies that no VLANs are inspected.
remove	(Optional) Removes the specified VLAN from NDP inspection.
all	(Optional) Inspects NDP traffic from all VLANs on the port.
vlan-id	(Optional) A specific VLAN on the interface. More than one VLAN can be specified. The VLAN number that can be used is from 1 to 4094.

Command Default

All NDP messages are inspected. Secure Neighbor Discovery (SeND) options are ignored. Neighbors are probed based on the criteria defined in the Neighbor Tracking feature. Per-port IPv6 address limit enforcement is disabled. Layer 2 header source MAC address validations are disabled. Per-port rate limiting of the NDP messages in software is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SY. The **limited-broadcast** keyword was deprecated.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The **limited-broadcast** keyword was deprecated.

Usage Guidelines

The **ipv6 nd inspection** command applies the NDP Inspection feature on a specified interface. If you enable the optional **attach-policy** or **vlan** keywords, NDP traffic is inspected by policy or by VLAN. If no VLANs are specified, NDP traffic from all VLANs on the port is inspected (which is equivalent to using the **vlan all** keywords).

If no policy is specified in this command, the default criteria are as follows:

- All NDP messages are inspected.
- SeND options are ignored.
- Neighbors are probed based on the criteria defined in neighbor tracking feature.
- Per-port IPv6 address limit enforcement is disabled.
- Layer 2 header source MAC address validations are disabled.
- Per-port rate limiting of the NDP messages in software is disabled.

If a VLAN is specified, its parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash (for example, **vlan 1-100,200,300-400**). Do not enter any spaces between comma-separated VLAN parameters or in dash-specified ranges.

Examples

The following example enables NDP inspection on a specified interface:

```
Router(config-if)# ipv6 nd inspection
```

ipv6 nd inspection policy

To define the neighbor discovery (ND) inspection policy name and enter ND inspection policy configuration mode, use the **ipv6 nd inspection** command in ND inspection configuration mode. To remove the ND inspection policy, use the **no** form of this command.

ipv6 nd inspection policy *policy-name*
no ipv6 nd inspection policy *policy-name*

Syntax Description

policy-name	The ND inspection policy name.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 nd inspection policy** command defines the ND inspection policy name and enters ND inspection policy configuration mode. Once you are in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **tracking**
- **trusted-port**
- **validate source-mac**

Examples

The following example defines an ND policy name as policy1:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
tracking	Overrides the default tracking policy on a port.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link-layer address.

ipv6 nd managed-config-flag

To set the "managed address configuration flag" in IPv6 router advertisements, use the **ipv6 nd managed-config-flag**command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

The following example configures the "managed address configuration flag" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
ipv6 nd prefix-advertisement	Configures which IPv6 prefixes are included in IPv6 router advertisements

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd na glean

To configure neighbor discovery (ND) to glean an entry from an unsolicited neighbor advertisement (NA), use the **ipv6 nd na glean** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean
no ipv6 nd na glean

Syntax Description

This command has no arguments or keywords.

Command Default

The router ignores an unsolicited NA.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

IPv6 nodes may choose to emit a multicast unsolicited NA packet following the successful completion of duplicate address detection (DAD). By default, these unsolicited NA packets are ignored by other IPv6 nodes. The **ipv6 nd na glean** command configures the router to create an ND entry on receipt of an unsolicited NA packet (assuming no such entry already exists and the NA has the link-layer address option). Use of this command allows a router to populate its ND cache with an entry for a neighbor in advance of any data traffic exchange with the neighbor.

Examples

The following example configures ND to glean an entry from an unsolicited neighbor advertisement:

```
Router(config-if)# ipv6 nd na glean
```

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation (NS) retransmissions on an interface, use the **ipv6 nd ns-interval**command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

Syntax Description

milliseconds	The interval between IPv6 neighbor solicit transmissions for address resolution. The acceptable range is from 1000 to 3600000 milliseconds.

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 (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

By default, using the **ipv6 nd ns-interval** command changes the NS retransmission interval for both address resolution and duplicate address detection (DAD). To specify a different NS retransmission interval for DAD, use the **ipv6 nd dad time**command.

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

Examples

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
ipv6 nd dad time	Configures the NS retransmit interval for DAD separately from the NS retransmit interval for address resolution.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd nud retry

To configure the number of times neighbor unreachability detection (NUD) resends neighbor solicitations (NSs), use the **ipv6 nd nud retry** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry *base interval max-attempts*
no ipv6 nd nud retry *base interval max-attempts*

Syntax Description

base	The base NUD value.
interval	The time interval, in milliseconds, between retries.
max-attempts	The maximum number of retry attempts, depending on the base value.

Command Default

Three NS packets are sent 1 second apart.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When a router runs NUD to re-resolve the ND entry for a neighbor, it sends three NS packets 1 second apart. In certain situations (for example, spanning-tree events, high traffic, the end host being reloaded), three NS packets sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for NS retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

tm

- *t* = Time interval
- *m* = Base (1, 2, or 3)
- *n* = Current NS number (where the first NS is 0)

The **ipv6 nd nud retry** command affects only the retransmit rate for NUD, not for initial resolution, which uses the default of three NS packets sent 1 second apart.

Examples

The following example provides a fixed interval of 1 second and three retransmits:

```
Router(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example provides a retransmit interval of 1, 2, 4, and 8:

```
Router(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example provides the retransmit intervals of 1, 3, 9, 27, 81:

```
Router(config-if)# ipv6 nd nud retry 3 1000 5
```

ipv6 nd other-config-flag

To set the "other stateful configuration" flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag**command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 nd other-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

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

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

Examples

The following example configures the "other stateful configuration" flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix

To configure IPv6 prefixes that are included in IPv6 Neighbor Discovery (ND) router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix {*ipv6-prefix/prefix-length* | **default**} [{**no-advertise** | [*valid-lifetime preferred-lifetime* [{**off-link** | **no-rtr-address** | **no-autoconfig** | **no-onlink**}]]}]
at *valid-date* | *preferred-date* [{**off-link** | **no-rtr-address** | **no-autoconfig**}]
no ipv6 nd prefix {*ipv6-prefix/prefix-length* | **default**}

Syntax Description

ipv6-prefix	Specifies the IPv6 network number to include in router advertisements (RA). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal format using 16-bit values between colons.
/ *prefix-length*	Specifies the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
default	Specifies that the default values are used.
no-advertise	(Optional) Specifies that the prefix is not advertised.
valid-lifetime	(Optional) Specifies the amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. The range is from 0 to 4294967295.
preferred-lifetime	(Optional) Specifies the amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. The range is from 0 to 4294967295.
off-link	(Optional) Configures the specified prefix as off-link. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a Connected prefix. If the prefix is already present in the routing table as a Connected prefix (for example, because the prefix was also configured using the **ipv6 address** command), then it will be removed.
no-rtr-address	(Optional) Indicates that the router will not send the full router address in prefix advertisements and will not set the R bit.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. The prefix will be advertised with the A-bit clear.
no-onlink	(Optional) Configures the specified prefix as not on-link. The prefix will be advertised with the L-bit clear.

at *valid-date*	(Optional) Specifies the date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Date is expressed in the form *date-valid-expire month-valid-expire year-valid-expire hh:mm-valid-expire*.
preferred-date	(Optional) Specifies the preferred expire date. Dates is expressed in the form *date-prefer-expire month-prefer-expire year-valid-expire hh:mm-prefer-expire*.

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Note that by default:

- All prefixes will be inserted in the routing table as Connected prefixes
- All prefixes will be advertised as on-link (for example, the L-bit will be set in the advertisement)
- All prefixes will be advertised as an autoconfiguration prefix (for example, the A-bit will be set in the advertisement)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **ipv6 nd prefix-advertisement** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(11)T	This command was modified. The **no-rtr-address** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(32.08.01)REC154	This command was modified. The **no-onlink** keyword was added.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

By default, prefixes configured as addresses on an interface using the **ipv6 address** command and additional prefixes configured using the **ipv6 nd prefix** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

If you configure the ND prefix using the **ipv6 nd prefix** command, both the interface IPv6 address and ND prefix is advertised.

Default Parameters

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

Prefix Lifetime and Expiration

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

On-Link

When on-link 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.

Autoconfiguration

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

The configuration options affect the L-bit and A-bit settings associated with the prefix in the IPv6 ND Router Advertisement, and presence of the prefix in the routing table, as follows:

- Default L=1 A=1 In Routing Table
- no-onlink L=0 A=1 In Routing Table
- no-autoconfig L=1 A=0 In Routing Table
- no-onlink no-autoconfig L=0 A=0 In Routing Table
- off-link L=0 A=1 Not in Routing Table
- off-link no-autoconfig L=0 A=0 Not in Routing Table

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

The following example advertises the prefix with the L-bit clear, so that the prefix is retained in the IPv6 routing table:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 address 2001::1/64
Device(config-if)# ipv6 nd prefix 2001::/64 3600 3600 no-onlink
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.

Command	Description
ipv6 mobile home-agent (interface configuration)	Initializes and starts the IPv6 Mobile home agent on a specific interface.
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix framed-ipv6-prefix

To add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue, use the **ipv6 nd prefix framed-ipv6-prefix**command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd prefix framed-ipv6-prefix
no ipv6 nd prefix framed-ipv6-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

Prefix is sent in the router advertisements (RAs).

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ipv6 nd prefix framed-ipv6-prefix**command to add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue and include it in RAs sent on the interface's link. By default, the prefix is sent in RAs. If the prefix in the attribute should be used by other applications such as the Dynamic Host Configuration Protocol (DHCP) for IPv6 server, administrators can disable the default behavior with the **no** form of the command.

Examples

The following example adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue:

```
ipv6 nd prefix framed-ipv6-prefix
```

ipv6 nd prefix-advertisement

Note Effective with Cisco IOS Release 12.2(13)T, the **ipv6 nd prefix-advertisement** command is replaced by the **ipv6 nd prefix** command. See the **ipv6 nd prefix** command for more information.

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix-advertisement**command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix-advertisement *ipv6-prefix/prefix-length valid-lifetime preferred-lifetime* [**onlink**] [**autoconfig**]
no ipv6 nd prefix-advertisement *ipv6-prefix/prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network number to include in router advertisements. 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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
valid-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred.
onlink	(Optional) Indicates that the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.
autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

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
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.

Release	Modification
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was replaced by the **ipv6 nd prefix** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Usage Guidelines

By default, prefixes configured on an interface using the **ipv6 address** command are advertised with "onlink" and "autoconfiguration" flags set. If you configure prefixes for advertisement using the **ipv6 nd prefix-advertisement**command, then only these prefixes are advertised.

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds, a preferred lifetime of 900 seconds, and both the "onlink" and "autoconfig" flags set:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd prefix-advertisement 2001:0DB8::/35 1000 900 onlink autoconfig
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 nd managed-config-flag	Sets the "managed address configuration" flag in IPv6 router advertisements.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra dns server

To configure the IPv6 router advertisement of DNS server addresses on an interface, use the **ipv6 nd ra dns server** command in interface configuration mode. To remove the IPv6 router advertisement of DNS server addresses, use the **no** form of this command.

ipv6 nd ra dns server *ipv6-address*
seconds
no ipv6 nd ra dns server *ipv6-address*

Syntax Description

seconds	The amount of time (in seconds) that the Domain Naming System (DNS) server is advertised in an IPv6 router advertisement (RA). The range is from 200 to 4294967295.

Command Default

The DNS server is not advertised in an IPv6 RA.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

You can use the **ipv6 nd ra dns server** command to configure up to eight DNS server addresses in an RA.

If you configure a *seconds* value of zero, the DNS server will no longer be used.

Example

The following example configures a DNS server with an IPv6 address of 2001:DB8:1::1 to be advertised in an RA with a lifetime of 600 seconds:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra dns server 2001:DB8:1::1 600
```

Related Commands

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

ipv6 nd ra interval

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

ipv6 nd ra interval {*maximum-secs* [*minimum-secs*] | **msec** *maximum-ms* [*minimum-ms*]}
no ipv6 nd ra interval

Syntax Description

maximum-secs	Maximum interval between IPv6 RA transmissions, in seconds. The range is from 4 to 1800.
minimum-secs	(Optional) Minimum interval between IPv6 RA transmissions, in seconds. The range is from 3 to 150.
msec	Specifies that the intervals are in milliseconds.
maximum-ms	Maximum interval between IPv6 RA transmissions, in milliseconds. The range is from 70 to 1800000.
minimum-ms	(Optional) Minimum interval between IPv6 RA transmissions, in milliseconds. The smallest possible RA interval is 30 milliseconds. The range is from 30 to 53.

Command Default

The default interval between IPv6 RA transmissions is 200 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ipv6 nd ra-interval** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.2(2)SA2	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using the **ipv6 nd ra lifetime** command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.

Users can explicitly configure a minimum RA interval. The minimum RA interval may never be more than 75 percent of the maximum RA interval and never less than 3 seconds (if specified in seconds). If the minimum RA interval is not configured, it is calculated as 75 percent of the maximum RA interval.

If the user specifies the time in milliseconds, then the minimum RA interval is 30 milliseconds. This limit allows configuration of very short RA intervals for Mobile IPv6.

The maximum and minimum RA intervals govern only unsolicited RA messages. Solicited RA messages are transmitted as router solicitation (RS) on the interface. However, if multiple RS messages are received every second, there is a minimum delay of 3 seconds between the RA messages. This limits the number of solicited RA messages transmitted from the interface.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 nd ra interval 201
```

The following examples shows a maximum RA interval of 200 seconds and a minimum RA interval of 50 seconds:

```
Device(config-if)# ipv6 nd ra interval 200 50
```

The following examples shows a maximum RA interval of 100 milliseconds and a minimum RA interval of 30 milliseconds, which is the smallest value allowed:

```
Device(config-if)# ipv6 nd ra interval msec 100 30
```

Related Commands

Command	Description
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.
ipv6 nd advertisement-interval	Configures the advertisement interval option to be sent in RAs.
ipv6 nd ra lifetime	Configures the router lifetime value in IPv6 router advertisements on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra lifetime

To configure the router lifetime value in IPv6 router advertisements on an interface, use the **ipv6 nd ra lifetime**command in interface configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra lifetime *seconds*
no ipv6 nd ra lifetime

Syntax Description

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

Command Default

The default lifetime value is 1800 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced. This command replaces the **ipv6 nd ra-lifetime** command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra lifetime 1801
```

Related Commands

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

ipv6 nd ra solicited unicast

To configure unified solicited Router Advertisement response method on an interface, use the **ipv6 nd ra solicited unicast** command in interface configuration mode. To remove solicited Router Advertisement response, use the **no** form of this command.

ipv6 nd ra solicited unicast
noipv6 nd ra solicited unicast

Syntax Description

There are no keywords or arguments for this command.

Command Default

The solicited Router Advertisement response is not configured.

Command Modes

Interface configuration

Command History

Release	Modification
15.4(2)T	This command was introduced.
15.4(2)S	This command was integrated into Cisco IOS Release 15.4(2)S.
15.2(1)SY1	This command was integrated into Cisco IOS Release 15.2(1)SY1.

Usage Guidelines

Large networks with a high concentration of mobile devices might experience like battery depletion, when solicited Router Advertisement messages are multicast . Use the **ipv6 nd ra solicited unicast** to unicast solicited Router Advertisement messages extend battery life of mobile device in the network.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra solicited unicast
```

Related Commands

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

ipv6 nd ra suppress

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

ipv6 nd ra suppress [**all**]
no ipv6 nd ra suppress

Syntax Description

all	(Optional) Suppresses all router advertisements (RAs) on an interface.

Command Default

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces 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
12.4(2)T	This command was introduced. This command replaces the **ipv6 nd suppress-ra**command.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **ipv6 nd ra suppress** command only suppresses periodic unsolicited RAs. It does not suppress RAs sent in response to a router solicitation. To suppress all RAs, including those sent in response to a router solicitation, use the **ipv6 nd ra suppress** command with the **all** keyword.

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

Examples

The following example suppresses IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra suppress
```

The following example enables the sending of IPv6 router advertisements on serial interface 0/1:

```
Router(config)# interface serial 0/1
Router(config-if)# no ipv6 nd ra suppress
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd raguard

To apply the router advertisements (RA) guard feature, use the **ipv6 nd raguard**command in interface configuration mode.

ipv6 nd raguard
no ipv6 nd raguard

Syntax Description

This command has no arguments or keywords.

Command Default

An RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.

Usage Guidelines

The **ipv6 nd raguard** command enables the RA guard feature. If the RA does not match with the configured option, the packet is dropped.

Examples

The following example applies the RA guard:

```
Router(config-if)# ipv6 nd raguard
```

ipv6 nd raguard attach-policy

To apply the IPv6 router advertisement (RA) guard feature on a specified interface, use the **ipv6 nd raguard attach-policy** command in interface configuration mode.

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3*...]]]

Syntax Description

policy-name	(Optional) IPv6 RA guard policy name.
vlan	(Optional) Applies the IPv6 RA guard feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from RA guard inspection.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3*...). The range of available VLAN numbers is from 1 through 4094.

Command Default

An IPv6 RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If no policy is specified using the *policy-name* argument, the port device role is set to host and all inbound router traffic (for example, RA and redirect messages) is blocked.

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the IPv6 RA guard feature is applied on GigabitEthernet interface 0/0:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguardpolicy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

Related Commands

Table 5:

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link layer address.

ipv6 nd reachable-time

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

ipv6 nd reachable-time *milliseconds*
no ipv6 nd reachable-time

Syntax Description

milliseconds	The amount of time that a remote IPv6 node is considered reachable (in milliseconds).

Command Default

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

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

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

Examples

The following example configures an IPv6 reachable time of 1,700,000 milliseconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd resolution data limit

To configure the number of data packets queued pending Neighbor Discovery resolution, use the **ipv6 nd resolution data limit** command in global configuration mode.

ipv6 nd resolution data limit *number-of-packets*
no ipv6 nd resolution data limit *number-of-packets*

Syntax Description

number-of-packets	The number of queued data packets. The range is from 16 to 2048 packets.

Command Default

Queue limit is 16 packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **ipv6 nd resolution data limit** command allows the customer to configure the number of data packets queued pending Neighbor Discovery resolution. IPv6 Neighbor Discovery queues a data packet that initiates resolution for an unresolved destination. Neighbor Discovery will only queue one packet per destination. Neighbor Discovery also enforces a global (per-router) limit on the number of packets queued. Once the global queue limit is reached, further packets to unresolved destinations are discarded. The minimum (and default) value is 16 packets, and the maximum value is 2048.

In most situations, the default value of 16 queued packets pending Neighbor Discovery resolution is sufficient. However, in some high-scalability scenarios in which the router needs to initiate communication with a very large number of neighbors almost simultaneously, then the value may be insufficient. This may lead to loss of the initial packet sent to some neighbors. In most applications, the initial packet is retransmitted, so initial packet loss generally is not a cause for concern. (Note that dropping the initial packet to an unresolved destination is normal in IPv4.) However, there may be some high-scale configurations where loss of the initial packet is inconvenient. In these cases, the customer can use the **ipv6 nd resolution data limit** command to prevent the initial packet loss by increasing the unresolved packet queue size.

Examples

The following example configures the global number of data packets held awaiting resolution to be 32:

```
Router(config)# ipv6 nd resolution data limit 32
```

ipv6 nd route-owner

To insert Neighbor Discovery-learned routes into the routing table with "ND" status and to enable ND autoconfiguration behavior, use the **ipv6 nd route-owner** command. To remove this information from the routing table, use the **no** form of this command.

ipv6 ndroute-owner

Syntax Description

This command has no arguments or keywords.

Command Default

The status of Neighbor Discovery-learned routes is "Static."

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

The **ipv6 nd route-owner** command inserts routes learned by Neighbor Discovery into the routing table with a status of "ND" rather than "Static" or "Connected."

This global command also enables you to use the **ipv6 nd autoconfig default** or **ipv6 nd autoconfig prefix** commands in interface configuration mode. If the **ipv6 nd route-owner** command is not issued, then the **ipv6 nd autoconfig default** and **ipv6 nd autoconfig prefix** commands are accepted by the router but will not work.

Examples

```
Device (config)# ipv6 nd route-owner
```

Related Commands

Command	Description
ipv6 nd autoconfig default	Allows Neighbor Discovery to install a default route to the Neighbor Discovery-derived default router.
ipv6 nd autoconfig prefix	Uses Neighbor Discovery to install all valid on-link prefixes from RAs received on the interface.

ipv6 nd router-preference

To configure a default router preference (DRP) for the router on a specific interface, use the **ipv6 nd router-preference**command in interface configuration mode. To return to the default DRP, use the **no** form of this command.

ipv6 nd router-preference {**high** | **medium** | **low**}
no ipv6 nd router-preference

Syntax Description

high	Preference for the router specified on an interface is high.
medium	Preference for the router specified on an interface is medium.
low	Preference for the router specified on an interface is low.

Command Default

Router advertisements (RAs) are sent with the **medium** preference.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

RA messages are sent with the DRP configured by the **ipv6 nd router-preference** command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Examples

The following example configures a DRP of high for the router on gigabit Ethernet interface 0/1:

```
Router(config)# interface Gigabit ethernet 0/1
Router(config-if)# ipv6 nd router-preference high
```

Related Commands

Command	Description
ipv6 nd ra interval	Configures the interval between IPv6 router advertisement transmissions on an interface.

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd secured certificate-db

To configure the maximum number of entries in an IPv6 Secure Neighbor Discovery (SeND) certificate database, use the **ipv6 nd secured certificate-db**command in global configuration mode. To disable any maximum number of entries set for a SeND certificate database, use the **no** form of this command.

ipv6 nd secured certificate-db max-entries *max-entries-value*
no ipv6 nd secured certificate-db max-entries

Syntax Description

max-entries *max-entries-value*	Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.

Command Default

No SeND certificate database is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

This command allows you to set up a maximum size for the certificate database (DB), to protect against denial of service (DoS) certificate flooding. When the limit is reached, new certificates are dropped.

The certificate DB is relevant on a router in host mode only, because it stores certificates received from routers.

Examples

The following example configures a SeND certificate database with a maximum number of 500 entries:

```
Router(config)# ipv6 nd secured certificate-db max-entries 500
```

Related Commands

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of entries that did not reach the destination in a SeND time-stamp database.

ipv6 nd secured full-secure

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a router, use the **ipv6 nd secured full-secure**command in global configuration mode. To disable SeND security mode, use the **no** form of this command.

ipv6 nd secured full-secure
no ipv6 nd secured full-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Non-SeND neighbor discovery messages are accepted by the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured full-secure** command in global configuration mode allows you to configure the router to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the specified router.

Examples

The following example enables SeND security mode on a router:

```
Router(config)# ipv6 nd secured full-secure
```

Related Commands

Command	Description
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.

ipv6 nd secured full-secure (interface)

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a specified interface, use the **ipv6 nd secured full-secure**command in interface configuration mode. To provide the co-existence mode for secure and nonsecure neighbor discovery messages on an interface, use the **no** form of this command.

ipv6 nd secured full-secure
no ipv6 nd secured full-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Non-SeND messages are accepted by the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured full-secure** command in interface configuration mode allows you to configure a specified interface to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the interface. If this command is not enabled, secure and nonsecure neighbor discovery messages can coexist on the same interface.

Examples

The following example enables SeND security mode on an interface:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured full-secure
```

Related Commands

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.

ipv6 nd secured key-length

To configure IPv6 Secure Neighbor Discovery (SeND) key-length options, use the **ipv6 nd secured key-length**command in global configuration mode. To disable the key length, use the **no** form of this command.

ipv6 nd secured key-length [[{**minimum** | **maximum**}] *value*]
no ipv6 nd secured key-length

Syntax Description

minimum *value*	(Optional) Sets the minimum key-length value, which should be at least 384 bits. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.
maximum *value*	(Optional) Sets the maximum key-length value. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.

Command Default

The key length is 1024 bits.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

When used by SeND, the key length is checked against the key-length value, as set in the **ipv6 nd secured key-length** command. When packets are received from a neighbor with a key length that is out of the configured boundaries, the packets are treated as unsecure.

Examples

The following example sets the minimum key-length value to 512 bits and the maximum value to 1024 bits:

```
Router(config)# ipv6 nd secured key-length minimum 512
Router(config)# ipv6 nd secured key-length maximum 1024
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of entries in a SeND time-stamp database.

ipv6 nd secured sec-level

To configure the minimum security value that IPv6 Secure Neighbor Discovery (SeND) will accept from its peer, use the **ipv6 nd secured sec-level**command in global configuration mode. To disable the security level, use the **no** form of this command.

ipv6 nd secured sec-level [**minimum** *value*]
no ipv6 nd secured sec-level

Syntax Description

minimum *value*	(Optional) Sets the minimum security level, which is a value from 0 through 7. The default security level is 1.

Command Default

The default security level is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured sec-level** command allows the user to configure the minimum security value the router will accept from its peer.

Examples

The following example sets the minimum security level to 2:

```
Router(config)# ipv6 nd secured sec-level 2
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of unreached entries in a SeND time-stamp database.

ipv6 nd secured timestamp

To configure the IPv6 Secure Neighbor Discovery (SeND) time stamp, use the **ipv6 nd secured timestamp**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 nd secured timestamp {**delta** *value* | **fuzz** *value*}
no ipv6 nd secured timestamp

Syntax Description

delta *value*	Specifies the maximum time difference accepted between the sender and the receiver. Default value is 300 seconds.
fuzz *value*	Specifies the maximum age of the message, when the delta is taken into consideration; that is, the amount of time, in seconds, that a packet can arrive after the delta value before being rejected. Default value is 1 second.

Command Default

Default time-stamp values are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured timestamp** command configures the amount of time the router waits before it accepts or rejects packets it has received.

Examples

The following example configures the SeND time stamp to be 600 seconds:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured timestamp delta 600
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp-db	Configures the maximum number of unreached entries in a SeND time-stamp database.

ipv6 nd secured timestamp-db

To configure the maximum number of unreached entries in an IPv6 Secure Neighbor Discovery (SeND) time-stamp database, use the **ipv6 nd secured timestamp-db**command in global configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 nd secured timestamp-db max-entries *max-entries-value*
no ipv6 nd secured timestamp-db max-entries

Syntax Description

max-entries *max-entries-value*	Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.

Command Default

No time-stamp database is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example configures the time-stamp database on a router:

```
Router(config)# ipv6 nd secured timestamp-db max-entries 345
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.

ipv6 nd secured trustanchor

To specify an IPv6 Secure Neighbor Discovery (SeND) trusted anchor on an interface, use the **ipv6 nd secured trustanchor**command in interface configuration mode. To remove a trusted anchor, use the **no** form of this command.

ipv6 nd secured trustanchor *trustanchor-name*
no ipv6 nd secured trustanchor *trustanchor-name*

Syntax Description

trustanchor-name	The name to be found in the certificate of the trustpoint.

Command Default

No trusted anchor is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured trustanchor**command is used to select the certificate authority (CA) you want to authenticate. The trusted anchors configured by this command act as as references to the trustpoints configured.

A crypto Public Key Infrastructure (PKI) trustpoint can be a self-signed root CA or a subordinate CA. The *trustpoint-name*argument refers to the name to be found in the certificate of the trustpoint.

The **ipv6 nd secured trustanchor**and **ipv6 nd secured trustpoint**commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands.

Examples

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustanchor anchor1
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
ipv6 nd secured trustpoint	Specifies which trustpoint should be used for selecting the certificate to advertise.

ipv6 nd secured trustpoint

To specify which trustpoint should be used in the ipv6 Secure Neighbor Discovery (SeND) protocol for selecting the certificate to advertise, use the **ipv6 nd secured trustpoint**command in interface configuration mode. To disable the trustpoint, use the **no** form of this command.

ipv6 nd secured trustpoint *trustpoint-name*
no ipv6 nd secured trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	The name to be found in the certificate of the trustpoint.

Command Default

SeND is not enabled on a specified interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured trustpoint** command enables SeND on an interface and specifies which trustpoint should be used. The trustpoint points to the Rivest, Shamir, and Adelman (RSA) key pair and the trusted anchor (which is the certificate authority [CA] signing your certificate).

The **ipv6 nd secured trustpoint** and **ipv6 nd secured trustanchor**commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands. However, the trustpoint provided in the **ipv6 nd secured trustpoint** command must include a router certificate and the signing CA certificate. It may also include the certificate chain up to the root certificate provided by a CA that hosts (connected to the router) will trust.

The trustpoint provided in the **ipv6 nd secured trustanchor** command must only include a CA certificate.

Examples

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustpoint trustpoint1
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
ipv6 nd secured trustanchor	Specifies a trusted anchor on an interface.

ipv6 nd suppress attach-policy

To apply the IPv6 neighbor discovery (ND) suppress feature on a specified interface, use the **ipv6 nd suppress attach-policy** command in interface configuration mode.

ipv6 nd suppress attach-policy [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

Syntax Description

policy-name	(Optional) IPv6 ND suppress policy name.
vlan	(Optional) Applies the IPv6 ND suppress feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from IPv6 ND suppression.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3...*). The range of available VLAN numbers is from 1 through 4094.

Command Default

An IPv6 ND suppress policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.3(1)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the IPv6 ND suppress feature is applied on Ethernet interface 0/0:

```
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy
```

Related Commands

Command	Description
ipv6 nd suppress policy	Enables IPv6 ND multicast suppress and enter ND suppress policy configuration mode

ipv6 nd suppress policy

To enable IPv6 Neighbor Discovery (ND) multicast suppress and enter ND suppress policy configuration mode, use the **ipv6 nd suppress policy** command in global configuration mode.

ipv6 nd suppress policy *policy-name*

Syntax Description

policy-name	IPv6 ND suppress policy name.

Command Default

An ND suppress policy is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(1)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 nd suppress policy** command to configure NA suppress globally on a device. After IPv6 ND suppress is configured globally, you can use the **ipv6 nd suppress attach-policy** command to enable IPv6 ND suppress on a specific interface.

Examples

The following example shows how to define the ND suppress policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)#
```

Related Commands

Command	Description
ipv6 nd suppress attach-policy	Applies the IPv6 ND suppress feature on a specified interface.

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 neighbor discovery cache, use the **no** form of this command.

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

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	The specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	The specified interface number.
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
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

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

Use the **show ipv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- INCMP (Incomplete)--The interface for this entry is down.
- REACH (Reachable)--The interface for this entry is up.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries. See the **show ipv6 neighbors**command for descriptions of the INCMP and REACH states for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor 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** command 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 INCMP).

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

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

Examples

The following example configures 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 1:

```
Router(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the ARP cache.
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
no ipv6 enable	Disables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
no ipv6 unnumbered	Disables IPv6 on an unnumbered interface.
show ipv6 neighbors	Displays IPv6 neighbor discovery cache information.

ipv6 neighbor binding

To change the defaults of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding [{**reachable-lifetime** *value* | **stale-lifetime** *value*}]
no ipv6 neighbor binding

Syntax Description

reachable-lifetime *value*	(Optional) The maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 through 3600 seconds, and the default is 300 seconds (or 5 minutes).
stale-lifetime *value*	(Optional) The maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).
down-lifetime *value*	(Optional) The maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).

Command Default

Reachable lifetime: 300 seconds Stale lifetime: 24 hours Down lifetime: 24 hours

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding** command to configure information about individual entries in a binding table. If no keywords or arguments are configured, the IPv6 neighbor binding entry defaults are used.

If the **tracking reachable-lifetime** command is configured, it overrides **ipv6 neighbor binding reachable-lifetime** configuration. If the **tracking stale-lifetime** command is configured, it overrides **ipv6 neighbor binding stale-lifetime** configuration.

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding reachable-entries 100
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.

Command	Description
tracking	Overrides the default tracking policy on a port.

ipv6 neighbor binding down-lifetime

To change the default of a neighbor binding entry's down lifetime, use the **ipv6 neighbor binding down-lifetime**command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding down-lifetime {*value* | **infinite**}
no ipv6 neighbor binding down-lifetime

Syntax Description

value	The maximum time, in minutes, an entry learned from a down interface is kept in the table before deletion. The range is from 1 to 3600 minutes. • The default is 24 hours (86,400 seconds).
infinite	Keeps an entry in the binding table for an infinite amount of time.

Command Default

A neighbor binding entry is down for 24 hours before it is deleted from the binding table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding down-lifetime**command to change the amount of time a neighbor binding is down before that binding is removed from the binding table.

Examples

The following example shows how to change a binding entry's down lifetime to 2 minutes before it is deleted from the binding table:

```
Router(config)# ipv6 neighbor binding down-lifetime 2
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding interface

To add a static entry to the binding table database for an interface, use the **ipv6 neighbor binding interface** command in global configuration mode. To remove the static entry, use the **no** form of this command.

ipv6 neighbor binding *IPv6-address* **interface** *type number*[{[*hardware-address*] | **tracking** [{**disable** | **enable** | **retry-interval** *seconds*}] | **reachable-lifetime** *seconds*}]
no ipv6 neighbor binding interface *type number*

Syntax Description

IPv6-address	IPv6 address of the static entry.
hardware-address	(Optional) Hardware address.
tracking	(Optional) Verifies a static entry's reachability directly.
disable	(Optional) Disables tracking for a particular static entry.
enable	(Optional) Enables tracking for a particular static entry.
retry-interval *seconds*	(Optional) Verifies a static entry's reachability, in seconds, at the configured interval. The range is from 1 to 3600, and the default is 300.
reachable-lifetime *seconds*	(Optional) Specifies the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery Protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 to 3600 seconds, and the default is 300 seconds.

Command Default

Static entries are not added to the binding table database for an interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The **ipv6 neighbor binding interface** command is used to control the content of the binding table. Use this command to add a static entry in the binding table database. The binding table manager is responsible for aging out entries and directly verifying their reachability by probing them (if the **tracking** keyword is enabled). Use of the **tracking** keyword overrides any general behavior provided globally by the **ipv6 neighbor tracking** command for this static entry. The **disable** keyword disables tracking for this static entry. The **reachable-lifetime** keyword defines the maximum time (300 seconds) that the entry will be kept once it is determined not to be reachable (or stale).

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1
reachable-lifetime 100
```

Related Commands

Command	Description
ipv6 neighbor binding max-entries	Specifies the maximum number of entries that are allowed to be inserted in the cache.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding logging

To enable the logging of binding table main events, use the **ipv6 neighbor binding logging** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 neighbor binding logging
no ipv6 neighbor binding logging

Syntax Description

This command has no arguments or keywords.

Command Default

Binding table events are not logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 neighbor binding logging** command enables the logging of the following binding table events:

- An entry is inserted into the binding table.
- A binding table entry was updated.
- A binding table entry was deleted from the binding table.
- A binding table entry was not inserted into the binding table, possibly because of a collision with an existing entry, or because the maximum number of entries has been reached.

Examples

The following example shows how to enable binding table event logging:

```
Router(config)# ipv6 neighbor binding logging
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.
ipv6 snooping logging packet drop	Configures IPv6 snooping security logging.

ipv6 neighbor binding max-entries

To specify the maximum number of entries that are allowed to be inserted in the binding table cache, use the **ipv6 neighbor binding max-entries** command in global configuration mode. To return to the default, use the **no** form of this command.

ipv6 neighbor binding max-entries *entries* [{**vlan-limit** *number* | **interface-limit** *number* | **mac-limit** *number*}]
no ipv6 neighbor binding max-entries *entries* [{**vlan-limit** | **mac-limit**}]

Syntax Description

entries	Number of entries that can be inserted into the cache.
vlan-limit *number*	(Optional) Specifies a neighbor binding limit per number of VLANs.
interface-limit *number*	(Optional) Specifies a neighbor binding limit per interface.
mac-limit *number*	(Optional) Specifies a neighbor binding limit per number of Media Access Control (MAC) addresses.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 neighbor binding max-entries** command is used to control the content of the binding table. This command specifies the maximum number of entries that are allowed to be inserted in the binding table cache. Once this limit is reached, new entries are refused, and the Neighbor Discovery Protocol (NDP) traffic source with the new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

The maximum number of entries can be set globally per VLAN, interface, or MAC addresses.

Examples

The following example shows how to specify globally the maximum number of entries inserted into the cache:

```
Router(config)# ipv6 neighbor binding max-entries 100
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding stale-lifetime

To set the length of time a stale entry is kept in the binding table, use the **ipv6 neighbor binding stale-lifetime**command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6 neighbor binding stale-lifetime {*value* | **infinite**}
no ipv6 neighbor binding

Syntax Description

value	The maximum time, in minutes, a stale entry is kept in the table before it is deleted or some proof of reachability is seen. The range is from 1 to 3600 minutes, and the default is 24 hours (or 1440 minutes).
infinite	Keeps an entry in the binding table for an infinite amount of time.

Command Default

Stale lifetime: 1440 minutes (24 hours)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding stale-lifetime**command to configure the length of time a stale entry is kept in the binding table before it is removed.

Examples

The following example shows how to change the stale lifetime for a binding entry to 720 minutes (or 12 hours):

```
Router(config)# ipv6 neighbor binding stale lifetime 720
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 neighbor binding vlan

To add a static entry to the binding table database, use the **ipv6 neighbor binding vlan** command in global configuration mode. To remove the static entry, use the **no** form of this command.

ipv6 neighbor binding vlan *vlan-id* {**interface** *type numberipv6-addressmac-address*} [{**tracking** [{**disable** | **enable** | **retry-interval** *value*}] | **reachable-lifetime** *value*}]
no ipv6 neighbor binding vlan *vlan-id*

Syntax Description

vlan-id	ID of the specified VLAN.
interface *type number*	Adds static entries by the specified interface type and number.
ipv6-address	IPv6 address of the static entry.
mac-address	Media Access Control (MAC) address of the static entry.
tracking	(Optional) Verifies a static entry's reachability directly.
disable	(Optional) Disables tracking for a particular static entry.
enable	(Optional) Enables tracking for a particular static entry.
retry-interval *value*	(Optional) Verifies a static entry's reachability, in seconds, at the configured interval. The range is from 1 to 3600, and the default is 300.
reachable-lifetime *value*	(Optional) Specifies the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery Protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 to 3600 seconds, and the default is 300 seconds.

Command Default

Retry interval: 300 seconds

Reachable lifetime: 300 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 neighbor binding vlan** command is used to control the content of the binding table. Use this command to add a static entry in the binding table database. The binding table manager is responsible for aging out entries and verifying their reachability directly by probing them (if the **tracking** keyword is enabled). Use of the **tracking** keyword overrides any general behavior provided globally by the **ipv6 neighbor tracking** command for this static entry. The **disable** keyword disables tracking for this static entry. The **stale-lifetime** keyword defines the maximum time the entry will be kept once it is determined to be not reachable (or stale).

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding vlan reachable-lifetime 100
```

Related Commands

Command	Description
ipv6 neighbor binding max-entries	Specifies the maximum number of entries that are allowed to be inserted in the cache.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor tracking

To track entries in the binding table, use the **ipv6 neighbor tracking** command in global configuration mode. To disable entry tracking, use the **no** form of this command.

ipv6 neighbor tracking [**retry-interval** *value*]
no ipv6 neighbor tracking [**retry-interval** *value*]

Syntax Description

retry-interval *value*	(Optional) Verifies a static entry's reachability at the configured interval time, in seconds, between two probings. The range is from 1 to 3600, and the default is 300.

Command Default

Entries in the binding table are not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 neighbor tracking** command enables the tracking of entries in the binding table. Entry reachability is tested at every interval configured by the optional **retry-interval** keyword (or every 300 seconds, which is the default retry interval) using the neighbor unreachability detection (NUD) mechanism used for directly tracking neighbor reachability.

Reachability can also be established indirectly by using Neighbor Discovery Protocol (NDP) inspection up to the VERIFY_MAX_RETRIES value (the default is 10 seconds). When there is no response, entries are considered stale and are deleted after the stale lifetime value is reached (the default is 1440 minutes).

When the **ipv6 neighbor tracking** command is disabled, entries are considered stale after the reachable lifetime value is met (the default is 300 seconds) and deleted after the stale lifetime value is met.

To change the default values of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command.

Examples

The following example shows how to track entries in a binding table:

```
Router(config)# ipv6 neighbor tracking
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 next-hop-self eigrp

To instruct a device configured with the Enhanced Interior Gateway Routing Protocol (EIGRP) that the IPv6 next hop is the local outbound interface address, use the **ipv6 next-hop-self eigrp** command in interface configuration mode. To instruct EIGRP to use the received next hop instead of the local outbound interface, use the **no** form of this command.

ipv6 next-hop-self eigrp *as-number*
no ipv6 next-hop-self eigrp *as-number*[{**no-ecmp-mode**}]

Syntax Description

as-number	Autonomous system number.
no-ecmp-mode	(Optional) Evaluates all paths to a network before advertising the paths out of an interface.

Command Default

The IPv6 next-hop-self state is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The **no-ecmp-mode** keyword was added.
Cisco IOS XE Release 3.5S	This command was modified. The **no-ecmp-mode** keyword was added.
15.2(3)T	This command was modified. The **no-ecmp-mode** keyword was added.

Usage Guidelines

EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out of the same interface on which they were learned. To change this default, use the **no ipv6 next-hop-self eigrp** command to instruct EIGRP to use the received next-hop value when advertising these routes. Some exceptions to this guideline are as follows:

- If your topology does not require spoke-to-spoke dynamic tunnels, you need not configure the **no ipv6 next-hop-self eigrp** command.
- If your topology requires spoke-to-spoke dynamic tunnels, you must use process switching on the tunnel interface on spoke devices. Otherwise, you will need to use a different routing protocol over Dynamic Multipoint VPN (DMVPN).

The **no-ecmp-mode** option is an enhancement to the **no ipv6 next-hop-self eigrp** command. When this option is enabled, all routes to a network in the EIGRP table are evaluated to check whether routes advertised from an interface were learned on the same interface. If a route advertised by an interface was learned on the same interface, the **no ipv6 next-hop-self eigrp** configuration is honored and the received next hop is used to advertise this route. Disabling the IPv6 next-hop self functionality is primarily useful in DMVPN spoke-to-spoke topologies.

Examples

The following example shows how to change the default IPv6 next-hop value by disabling the **ipv6 next-hop-self** functionality and configuring EIGRP to use the received next-hop value to advertise routes:

```
Device(config)# interface serial 0
Device(config-if)# no ipv6 next-hop-self eigrp 1 no-ecmp-mode
```

Related Commands

Command	Description
next-hop-self	Instructs an EIGRP device that the IPv6 next hop is the local outbound interface.
ip next-hop-self eigrp	Enables EIGRP to advertise routes with the local outbound interface address as the next hop.

ipv6 nhrp authentication

To configure the authentication string for an interface using the Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication**command ininterface configuration mode. To remove the authentication string, use the **no** form of this command.

ipv6 nhrp authentication *string*
no ipv6 nhrp authentication [*string*]

Syntax Description

string	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.

Command Default

No authentication string is configured. Cisco IOS software adds no authentication option to NHRP packets it generates.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

All routers configured with NHRP within one logical nonbroadcast multiaccess (NBMA) network must share the same authentication string.

Examples

In the following example, the authentication string named examplexx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ip nhrp authentication examplexx
```

ipv6 nhrp cache non-authoritative

To make a hub non-authoritative to respond to resolution requests, use the **ipv6 nhrp cache non-authoritative** command.

To make a hub authoritative to respond to resolution requests, use the **no** form of the command.

ipv6 nhrp cache non-authoritative

no ipv6 nhrp cache non-authoritative

Command Default

By default this command is configured and the hub is non-authoritative to respond to resolution requests.

Command Modes

Interface configuration

Command History

Release	Modification
IOS XE Release 16.8.1	Command introduced.

Example

```
interface tunnel0
  no ipv6 nhrp cache non-authoritative
```

ipv6 nhrp holdtime

To change the number of seconds that Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ipv6 nhrp holdtime**command ininterface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nhrp holdtime *seconds*
no ipv6 nhrp holdtime [*seconds*]

Syntax Description

seconds	Time, in seconds, that NBMA addresses are advertised as valid in positive authoritative NHRP responses.

Command Default

7200 seconds (2 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **ipv6 nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IPv6-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

Examples

In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
ipv6 nhrp holdtime 3600
```

ipv6 nhrp interest

To control which IPv6 packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ipv6 nhrp interest**command ininterface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nhrp interest *ipv6-access-list*
no ipv6 nhrp interest [*ipv6-access-list*]

Syntax Description

ipv6-access-list	IPv6 access list number in the range from 1 to 199.

Command Default

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **ipv6 nhrp interest** command with the **ipv6 access-list** command to control which IPv6 packets trigger NHRP requests.

Examples

In the following example, the IPv6 packets specified by the IPv6 access list named list2 will trigger NHRP requests:

```
Router(config)# ipv6 access-list list2
permit any any
Router(config-if)# ipv6 nhrp interest list2
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.

ipv6 nhrp map

To statically configure the IPv6-to-nonbroadcast multiaccess (NBMA) address mapping of IPv6 destinations connected to an NBMA network, use the **ipv6 nhrp map** command in interface configuration mode. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

ipv6 nhrp map *ipv6-address nbma-address* [**preference** *pref*]
no ipv6 nhrp map *ipv6-address nbma-address* [**preference** *pref*]

Syntax Description

ipv6-address	IPv6 address of the destination reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	An IPv4 or IPv6 NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a network service access point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address.
preference *pref*	(Optional) Assigns a preference for the IP-to-NBMA address mapping. The preference must be in the range 1 to 255.

Command Default

No static IPv6-to-NBMA cache entries exist.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.2(1)T	This command was modified. The *nbma-address* argument was enhanced to support IPv4 and IPv6 addresses.
Cisco IOS XE Release 16.8.1	This command was modified. Option to assign a preference for IP-to-NBMA address mapping was added.

Usage Guidelines

The **ipv6 nhrp map** command accepts IPv6 prefixes in the form of **prefix/** *prefix-length*, as shown in the following example:

```
ipv6 nhrp map abcd::abcd/128 172.16.1.1
```

Because the NBMA supports IPv4 addresses, only IPv4 destinations are accepted in the **ipv6 nhrp map** command. IPv6 prefixes can be mapped to IPv4 addresses.

You will probably need to configure at least one static mapping in order to reach the next hop server. Repeat this command to statically configure multiple IPv6-to-NBMA address mappings.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next hop servers 2001:0DB8:3333:4::5 and 2001:0DB8:4444:5::6. The NBMA address for 2001:0DB8:3333:4::5 is statically configured to be 2001:0DB8:5555:5::6 and the NBMA address for 2001:0DB8:4444:5::6 is 2001:0DB8:8888:7::6.

```
interface tunnel 0
 ipv6 nhrp nhs 2001:0DB8:3333:4::5
 ipv6 nhrp nhs 2001:0DB8:4444:5::6
 ipv6 nhrp map 2001:0DB8:3333:4::5 10.1.1.1 preference 3
 ipv6 nhrp map 2001:0DB8:4444:5::6 10.2.2.2 preference 9
```

ipv6 nhrp map multicast

To map destination IPv6 addresses to IPv4 nonbroadcast multiaccess (NBMA) addresses, use the **ipv6 nhrp map multicast**command in interface configuration mode. To remove the destination IPv6 addresses, use the **no** form of this command.

ipv6 nhrp map multicast {*ipv4-nbma-addressipv6-nbma-address*}
no ipv6 nhrp map multicast {*ipv4-nbma-addressipv6-nbma-address*}

Syntax Description

ipv4-nbma-address	IPv4 NBMA address (IPv6 over IPv4 transport) that is directly reachable through the NBMA network.
ipv6-nbma-address	IPv6 NMBA address that is directly reachable through the NBMA network.

Command Default

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.2(1)T	This command was modified. Support was extended to IPv6 NBMA addresses.

Usage Guidelines

The **ipv6 nhrp map multicast**command works only with tunnel interfaces.

The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IPv4 multicasts. If the underlying network supports IPv4 multicasts, you should use the **tunnel destination** command to configure a multicast destination for the transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, an IPv6 address is mapped to the IPv4 address 10.11.11.99:

```
ipv6 nhrp map 2001:0DB8::99/128 10.11.11.99
 ipv6 nhrp map multicast 10.11.11.99
```

Related Commands

Command	Description
tunnel destination	Specifies the destination for a tunnel interface.

ipv6 nhrp map multicast dynamic

To allow Next Hop Resolution Protocol (NHRP) to automatically add routers to the multicast NHRP mappings , use the **ipv6 nhrp map multicast dynamic**command in interface configuration mode. To disable this functionality, use the **no** form of this command

ipv6 nhrp map multicast dynamic
no ipv6 nhrp map multicast dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

Routers are not automatically added to the multicast NHRP mapping.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **ipv6 nhrp map multicast dynamic** command when spoke routers need to initiate multipoint generic routing encapsulation (GRE) and IP security (IPsec) tunnels and register their unicast NHRP mappings. This command is needed to enable dynamic routing protocols to work over the Multipoint GRE and IPsec tunnels because IGP routing protocols use multicast packets. This command prevents the hub router from needing a separate configuration line for a multicast mapping for each spoke router.

Examples

The following example shows how to enable the **ipv6 nhrp map multicast dynamic**command on the hub router:

```
crypto ipsec profile cisco-ipsec
 set transform-set cisco-ts
!
interface Tunnel0
 bandwidth 100000
 ip address 10.1.1.99 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 delay 50000
 ipv6 address 2001:0DB8::99/100
 ipv6 address FE80::0B:0B:0B:8F link-local
 ipv6 enable
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 no ipv6 next-hop-self eigrp 1
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 99
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile cisco-ipsec
```

Related Commands

Command	Description
ipv6 nhrp network-id	Enables NHRP on an interface.

ipv6 nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ipv6 nhrp max-send**command in interface configuration mode. To restore this frequency to the default value, use the **no** form of this command.

ipv6 nhrp max-send *pkt-count* **every** *seconds*
no ipv6 nhrp max-send

Syntax Description

pkt-count	Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
every *seconds*	Specifies the time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Command Default

Maximum frequency default settings are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The software maintains a per-interface quota of NHRP packets that can be sent. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the *seconds*argument:

- The user needs to consider the number of spoke routers being handled by this hub and how often they send NHRP registration requests. To support this load you would need:

Number of spokes / registration timeout * *max-send-interval*

- • Example:

500 spokes with 100-second registration timeout

Max send value = 500/100*10 = 50

- The maximum number of spoke-spoke tunnels that are expected to be up at any one time across the whole DMVPN network.

spoke-spoke tunnels/NHRP holdtime * max-send-interval

This formula covers spoke-spoke tunnel creation and the refreshing of spoke-spoke tunnels that are used for longer periods of time:

- • Example

2000 spoke-spoke tunnels with 250-second hold timeout

Max send value = 2000/250*10 = 80

Then add these together and multiply this by 1.5 to 2.0 to give a buffer:

- • Example

Max send = (50 + 80) * 2 = 260

- The max-send interval can be used to keep the long-term average number of NHRP messages allowed to be sent constant, but to allow greater peaks:
    - Example

400 messages in 10 seconds

In this case, it could peak at approximately 200 messages in the first second of the 10-second interval, but still keep to a 40-messages-per-second average over the 10-second interval:

4000 messages in 100 seconds

In this case, it could peak at approximately 2000 messages in the first second of the 100-second interval, but it would still be held to 40-messages-per-second average over the 100-second interval. In the second case, it could handle a higher peak rate, but risk a longer period of time when no messages can be sent if it used up its quota for the interval.

By default, the maximum rate at which the software sends NHRP packets is five packets per 10 seconds. The software maintains a per-interface quota of NHRP packets (whether generated locally or forwarded) that can be sent.

Examples

In the following example, only one NHRP packet can be sent from serial interface 0 each minute:

```
interface serial 0
 ipv6 nhrp max-send 1 every 60
```

Related Commands

Command	Description
ipv6 nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ipv6 nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ipv6 nhrp multicast

To configure multicast batch size and batch interval, use the **ipv6 nhrp multicast** command in interface configuration mode. To remove the multicast batch size and batch interval configuration, use the **no** form of this command.

ipv6 nhrp multicast [**batch-size** *num*][**batch-interval** *milliseconds*]

no ipv6 nhrp multicast [**batch-size** *num*][**batch-interval** *milliseconds*]

Syntax Description

batch-size *num*	Specifies the batch size of multicast replication.
batch-interval *milliseconds*	Specifies the interval for batch multicast replication.

Command Default

The default multicast batch-size is 250. The default multicast batch-interval is 10 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
IOS XE Release 16.8.1	Command introduced.

Example

The following example shows the multicast batch-size configured to 12 and the batch-interval configured to 10 milliseconds for a tunnel interface.

```
interface tunnel0
 ipv6 nhrp multicast batch-size 12 batch-interval 10
```

ipv6 nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ipv6 nhrp network-id**command ininterface configuration mode. To disable NHRP on the interface, use the **no** form of this command..

ipv6 nhrp network-id *network-id*
no ipv6 nhrp network-id *network-id*

Syntax Description

network-id	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.

Command Default

NHRP is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.

Examples

The following example shows how to enablle NHRP on the interface:

```
Router(config-if)# ipv6 nhrp network-id 99
```

Related Commands

Command	Description
ipv6 nhrp map multicast dynamic	Allows NHRP to automatically add routers to the multicast NHRP mappings.

ipv6 nhrp nhs

To specify the IPv6 prefix of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ipv6 nhrp nhs**command ininterface configuration mode. To remove the prefix address, use the **no** form of this command.

ipv6 nhrp nhs { *ipv6-nhs-address* [**scope** { *global* }] [**nbma** { *nbma-address fqdn-string* }] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic** [**scope** { *global* }] **nbma** { *nbma-address fqdn-string* } [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}
no ipv6 nhrp nhs {*ipv6-nhs-address* [**scope** { *global* }][**nbma** {*nbma-addressfqdn-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic** [**scope** { *global* }] **nbma** {*nbma-addressfqdn-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

Syntax Description

ipv6-nhs-address	IPv6 prefix of the next hop server being specified.
nbma	(Optional) Specifies nonbroadcast multiple access (NBMA) values.
nbma-address	(Optional) IPv4 or IPv6 NBMA address.
fqdn-string	(Optional) Next hop address (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255, where 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10, where 0 is the highest and 10 is the lowest value. The default value is 0.
max-connections *value*	Specifies the number of NHS elements from each NHS group that need to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.
scope *global*	Defines the scope for the NHS address. The default behaviour is to register with both global unicast and link local address. If the scope is set to *global*, the registration is limited to global unicast address only.

Command Default

No next hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.1(2)T	This command was modified. The *net-address* argument was removed and the **nbma**, *nbma-address*, *fqdn-string*, **multicast**, **priority** *value*, **cluster** *value*, **max-connections** *value*, **dynamic**, and **fallback** *seconds* keywords and arguments were added.
15.2(1)T	This command was modified. The *nbma-address* argument was modified to support IPv4 addresses.

Usage Guidelines

Use the **ipv6 nhrp nhs** command to specify the IPv6 prefix of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop IPv6 prefixes override the forwarding path that would otherwise be used for NHRP traffic.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address*argument, but with different IPv6 network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ipv6 nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ipv6 nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 priority 1 cluster 2
```

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IP-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.
show ipv6 nhrp	Displays NHRP mapping information.

ipv6 nhrp record

To reenable the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ipv6 nhrp record**command in interface configuration mode. To suppress the use of such options, use the **no** form of this command.

ipv6 nhrp record
no ipv6 nhrp record

Syntax Description

This command has no arguments or keywords.

Command Default

Forward record and reverse record options are used in NHRP request and reply packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ipv6 nhrp responder**command.

Examples

The following example suppresses forward record and reverse record options:

```
no ipv6 nhrp record
```

Related Commands

Command	Description
ipv6 nhrp responder	Designates the primary IP address of which interface the next hop server will use in NHRP reply packets when the NHRP requester uses the Responder Address option.

ipv6 nhrp redirect

To enable Next Hop Resolution Protocol (NHRP) redirect, use the **ipv6 nhrp redirect**command in interface configuration mode. To remove the NHRP redirect, use the **no** form of this command.

ipv6 nhrp redirect [**timeout** *seconds*]
no ipv6 nhrp redirect [**timeout** *seconds*]

Syntax Description

timeout *seconds*	(Optional) Indicates the interval, in seconds, that the NHRP redirects are sent for the same nonbroadcast multiaccess (NBMA) source and destination combination. The range is from 2 to 30 seconds.

Command Default

NHRP redirect is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The NHRP redirect message is an indication that the current path to the destination is not optimal. The receiver of the message should find a better path to the destination.

This command generates an NHRP redirect traffic indication message if the incoming and outgoing interface is part of the same dynamic multipoint VPN (DMVPN) network. The NHRP shortcut switching feature depends on receiving the NHRP redirect message. NHRP shortcut switching does not trigger an NHRP resolution request on its own. It triggers an NHRP resolution request only after receiving an NHRP redirect message.

Most of the traffic would follow a spoke-hub-spoke path. NHRP redirect is generally required to be configured on all the DMVPN nodes in the event the traffic follows a spoke-spoke-hub-spoke path.

Do not configure this command if the DMVPN network is configured for full-mesh. In a full-mesh configuration, the spokes are populated with a full routing table, with the next hop being the other spokes.

Examples

The following example shows how to enable NHRP redirects on the interface:

```
ipv6 nhrp redirect
```

Related Commands

Command	Description
ipv6 nhrp shortcut	Enables NHRP shortcut switching.

ipv6 nhrp registration

To enable the client to set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ipv6 nhrp registration** command in interface configuration mode. To reenable this functionality, use the **no** form of this command.

ipv6 nhrp registration [{**timeout** *seconds* | **no-unique** | **req-def-map**}]
no ipv6 nhrp registration [{**timeout** *seconds* | **no-unique** | **req-def-map**}]

Syntax Description

timeout *seconds*	(Optional) Specifies the time between periodic registration messages: • *seconds* --Number of seconds. The range is from 1 through the value of the NHRP hold timer. • If the **timeout** keyword is not specified, NHRP registration messages are sent every number of seconds equal to one-third the value of the NHRP hold timer.
no-unique	(Optional) Enables the client to not set the unique flag in the NHRP request and reply packets.
req-def-map	(Optional) Enables the client to request default maps in registration.

Command Default

The default settings are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 16.10.1	The **req-def-map** keyword was added.

Usage Guidelines

If the unique flag is set in the NHRP registration request packet, a next hop server (NHS) must reject any registration attempts for the same private address using a different nonbroadcast multiaccess (NBMA) address. If a client receives a new IP address-for example, via DHCP-and tries to register before the cache entry on the NHS times out, the NHS must reject it.

By configuring the **ip nhrp registration** command and **no-unique** keyword, the unique flag is not set, and the NHS can override the old registration information.

This command and keyword combination is useful in an environment where client IPv6 addresses can change frequently such as a dial environment.

By configuring the **ip nhrp registration** command and the **req-def-map** keyword, the NHRP client requests for default map from the server via registration message.

Examples

The following example configures the client not to set the unique flag in the NHRP registration packet:

```
interface FastEthernet 0/0
 ipv6 nhrp registration no-unique
```

The following example shows that the registration timeout is set to 120 seconds, and the delay is set to 5 seconds:

```
interface FastEthernet 0/0
 ipv6 nhrp registration 120 5
```

The following example configures the client to enable requesting default maps in registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration req-def-map
```

Related Commands

Command	Description
ipv6 nhrp holdtime	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses

ipv6 nhrp resolution refresh base

The default NHRP resolution requests follow the routed path to the destination spoke (exit point out the DMVPN cloud). For the first resolution request, this routed path is via the hub(s) all the way to the destination spoke. Owing to the on-demand route created as a result of the resolution process, for a resolution request sent for refreshing on-demand spoke-spoke routes and tunnels the routed path is the direct path between the spokes. This revalidates the direct spoke-spoke path like a keepalive and also reduces the load on the hub.

You can use this command to make the requests follow the base routed path via the hub(s), and do not take the on-demand path/route that was learnt for the prefix/next hop.

ipv6 nhrp resolution refresh base *number*
no ipv6 nhrp resolution refresh base

Syntax Description

refresh	Displays resolution refresh-related configuration options.
base	Configures the base routed path for routing resolution requests for refresh. This excludes the on-demand/shortcut routed path for routing resolution requests for refreshes.
number	(Optional) Specifies which refresh goes through the base path.

Command Default

The default settings are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 17.4 Release	The **refresh** and **base** keywords were introduced to the **ipv6 nhrp resolution refresh base** command.

Usage Guidelines

Use **ipv6 nhrp resolution refresh base** *number* on the tunnel interface on the spoke when it is intended that the resolution requests follow the base routed path via the hub(s) and don’t take the on-demand path/route that was learnt for the prefix/next hop. When configured, it should be configured symmetrically at both ends, else, it leads to asymmetric behavior.

Examples

The following example displays what the *number* denotes:

- When the value is n=1, every refresh goes through the base path.
- When the value is n=2, every second refresh goes through the base path, while other values still follow the default behaviour.

```
ipv6 nhrp resolution refresh base 1
```

Related Commands

Command	Description
ipv6 nhrp send-routed	This command is enabled by default and is used to forward the resolution requests via the routed path.

Command	Description
no ipv6 nhrp send-routed	This command causes NHRP control packets to be sent over the routed path to the destination/next hop. This is enabled by default.

ipv6 nhrp responder

To designate the primary IPv6 address the next hop server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ipv6 nhrp responder**command ininterface configuration mode. To remove the designation, use the **no** form of this command.

ipv6 nhrp responder *interface-type interface-number*
no ipv6 nhrp responder [*interface-type*] [*interface-number*]

Syntax Description

interface-type	Interface type whose primary IPv6 address is used when a next hop server complies with a Responder Address option (for example, **serial** or **tunnel**).
interface-number	Interface number whose primary IPv6 address is used when a next hop server complies with a Responder Address option.

Command Default

The next hop server uses the IPv6 address of the interface where the NHRP request was received.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If an NHRP requestor wants to know which next hop server generates an NHRP reply packet, it can request that information through the Responder Address option. The next hop server that generates the NHRP reply packet then complies by inserting its own IPv6 address in the Responder Address option of the NHRP reply. The next hop server uses the primary IPv6 address of the specified interface.

If an NHRP reply packet being forwarded by a next hop server contains the IPv6 address of that next hop server, the next hop server generates an Error Indication of type "NHRP Loop Detected" and discards the reply packet.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a next hop server to supply the primary IPv6 address of serial interface 0 in the NHRP reply packet:

```
ipv6 nhrp responder serial 0
```

ipv6 nhrp send-routed

To forward the resolution requests via the routed path, use **ipv6 nhrp send-routed** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nhrp send-routed
no ipv6 nhrp send-routed

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
16.9	This command was introduced.

Usage Guidelines

With **ipv6 nhrp send-routed** configured, the control packets take the routed path instead of nhs priority path. Without send-routed, the nhs priority configuration takes effect. The path taken by the control packets can be verfied using **show ipv6 nhrp traffic** command.

For all non-registration packets, the first NHRP resolution request takes the route installed by the IGP initially and then is forwarded along the routed path, for subsequent requests. The routed path can be the NHRP route or NHOs.

If the routed path fails for some reasons, tunnel falls back to the NHS path.

Examples

The following is an example of tunnel interface when the tunnel interface is disabled:

```
interface Tunnel0
 ipv6 address 2001::2/64
 ipv6 enable
 ipv6 nhrp authentication test
 ipv6 nhrp map 3001::2/64 10.1.1.2
 ipv6 nhrp network-id 100
 no ipv6 nhrp send-routed
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
```

ipv6 nhrp server-only

To configure the interface to operate in Next Hop Resolution Protocol (NHRP) server-only mode, use the **ipv6 nhrp server-only**command ininterface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nhrp server-only [**non-caching**]
no ipv6 nhrp server-only

Syntax Description

non-caching	(Optional) Specifies that the router will not cache NHRP information received on this interface.

Command Default

The interface does not operate in NHRP server-only mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut Switched Virtual Circuit (SVC).

Examples

The following example shows that the interface is configured to operate in server-only mode:

```
ipv6 nhrp server-only
```

ipv6 nhrp shortcut

To enable Next Hop Resolution Protocol (NHRP) shortcut switching, use the **ipv6 nhrp shortcut**command in interface configuration mode. To remove shortcut switching from NHRP, use the **no** form of this command.

ipv6 nhrp shortcut
no ipv6 nhrp shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

NHRP shortcut switching is disabled.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Do not configure this command if the dynamic multipoint VPN (DMVPN) network is configured for full-mesh. In a full-mesh configuration, the spokes are populated with a full routing table, with the next hop being the other spokes.

Examples

The following example shows how to configure an NHRP shortcut on an interface:

```
Router(config-if)# ipv6 nhrp shortcut
```

Related Commands

Command	Description
ipv6 nhrp redirect	Enables NHRP redirect.

ipv6 nhrp trigger-svc

To configure when the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ipv6 nhrp trigger-svc**command ininterface configuration mode. To restore the default thresholds, use the **no** form of this command.

ipv6 nhrp trigger-svc *trigger-threshold teardown-threshold*
no ipv6 nhrp trigger-svc

Syntax Description

trigger-threshold	Average traffic rate calculated during the load interval, at or above which NHRP will set up an SVC for a destination. The default value is 1 kb/s.
teardown-threshold	Average traffic rate calculated during the load interval, at or below which NHRP will tear down the SVC to the destination. The default value is 0 kb/s.

Command Default

The SVC default settings are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The two thresholds are measured during a sampling interval of 30 seconds, by default.

Examples

In the following example, the triggering and teardown thresholds are set to 100 kb/s and 5 kb/s, respectively:

```
ipv6 nhrp trigger-svc 100 5
```

ipv6 nhrp use

To configure the software so that the Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ipv6 nhrp use**commandininterface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nhrp use *usage-count*
no ipv6 nhrp use *usage-count*

Syntax Description

usage-count	Packet count in the range from 1 to 65535. Default is 1.

Command Default

The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

When the software attempts to send a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination normally is sent immediately. Configuring the *usage-count*argument causes the system to wait until the configured number of data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 2001:0DB8:3333:4::5 and one packet toward 2001:0DB8:5555:5::6, then an NHRP request is generated for 2001:0DB8:3333:4::5 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests is performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ipv6 nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the ipv6 nhrp use command controls *how readily* the system attempts such address resolution.

Examples

In the following example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

```
ipv6 nhrp use 5
```

Related Commands

Command	Description
ipv6 nhrp interest	Controls which IPv6 packets can trigger sending an NHRP request.
ipv6 nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

ipv6 ospf area

To enable Open Shortest Path First version 3 (OSPFv3) on an interface, use the **ip v6 ospf area** command in interface configuration mode. To disable OSPFv3 routing for interfaces defined, use the **no** form of this command.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]
no ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

Syntax Description

process-id	Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process.
area-id	Area that is to be associated with the OSPFv3 interface.
instance instance-id	(Optional) Instance identifier.

Command Default

OSPFv3 is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)S	Use of the **ospfv3 area**command can affect the **ipv6 ospf area** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 area**command can affect the **ipv6 ospf area** command.
15.2(1)T	Use of the **ospfv3 area**command can affect the **ipv6 ospf area** command.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

If the **ospfv3 area**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf area** configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

Before you enable OSPFv3 on an interface using the **ipv6 ospf area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

An OSPFv3 instance (also known as an OSPFv3 process) can be considered a logical device running OSPFv3 in a physical device. Use the instance ID to control selection of other devices as your neighbors. You become neighbors only with devices that have the same instance ID.

In IPv6, users can configure many addresses on an interface. In OSPFv3, all addresses on an interface are included by default. Users cannot select some addresses to be imported into OSPFv3; either all addresses on an interface are imported, or no addresses on an interface are imported.

There is no limit to the number of **ipv6 ospf area** commands you can use on the device. You must have at least two interfaces configured for OSPFv3 to run.

Examples

The following example enables OSPFv3 on an interface:

```
ipv6 unicast-routing
interface ethernet0/1
  ipv6 enable
  ipv6 ospf 1 area 0
ipv6 unicast-routing
interface ethernet0/2
  ipv6 enable
  ipv6 ospf 120 area 1.4.20.9 instance 2
```

Related Commands

Command	Description
ipv6 router ospf	Enables OSPFv3 router configuration mode.
ospfv3 area	Enables an OSPFv3 instance with the IPv4 or IPv6 address family.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf authentication

To specify the authentication type for an Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 ospf authentication** command in interface configuration mode. To remove the authentication type for an interface, use the **no** form of this command.

ipv6 ospf authentication {**null** | **ipsec spi** *spi* *authentication-algorithm* [*key-encryption-type*] [*key*]}
no ipv6 ospf authentication ipsec spi *spi*

Syntax Description

ipsec	Specifies IP Security (IPsec).
spi *spi*	Specifies the security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295, which is entered as a decimal.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5** —Enables message digest 5 (MD5) authentication. • **sha1** —Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	(Optional) One of two values can be entered: • **0** —The key is not encrypted. • **7** —The key is encrypted.
key	Number used in the calculation of the message digest. When MD5 authentication is used, the key must be 32 hexadecimal digits (16 bytes) long. When SHA-1 authentication is used, the key must be 40 hexadecimal digits (20 bytes) long.
null	Overrides area authentication.

Command Default

No authentication.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	This command was modified. The **sha1** keyword was added.
15.1(3)S	This command was modified. Use of the **ospfv3 authentication** command can affect the **ipv6 ospf authentication** command.
Cisco IOS XE Release 3.4S	This command was modified. Use of the **ospfv3 authentication** command can affect the **ipv6 ospf authentication** command.

Release	Modification
15.2(1)T	This command was modified. Use of the **ospfv3 authentication** command can affect the **ipv6 ospf authentication** command.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

You need to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a device. This means that two IPsec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **ipv6 ospf authentication null** command.

Beginning with Cisco IOS Release 12.4(4)T, the **sha1** keyword can be used to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is considered to be somewhat more secure than the MD5 algorithm, and it requires a 40-hexadecimal-digit (20-byte) key rather than the 32-hexadecimal-digit (16-byte) key that is required for MD5 authentication.

Examples

The following example shows how to enable MD5 authentication and then override area authentication:

```
Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef
Router(config-if)# ipv6 ospf authentication null
```

The following example shows how to enable SHA-1 authentication on the interface:

```
Router(config)# interface Ethernet0/0
Router(config)# ipv6 enable
Router(config-if)# ipv6 ospf authentication ipsec spi 500 sha1
1234567890123456789012345678901234567890
```

Related Commands

Command	Description
ipv6 router ospf	Enables OSPF router configuration mode.
ospfv3 authentication	Specifies the authentication type for an OSPFv3 instance.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Open Shortest Path First version 3 (OSPFv3), use the **ipv6 ospf bfd**command in interface configuration mode.To remove the **ospf bfd** command, use the **no** form of this command.

ipv6 ospf bfd [**disable**]
no ipv6 ospf bfd

Syntax Description

disable	(Optional) Disables BFD for OSPFv3 on a specified interface.

Command Default

When the **disable** keyword is not used, the default behavior is to enable BFD support for OSPFv3 on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(3)S	Use of the **ospfv3 bfd**command can affect the **ipv6 ospf bfd**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 bfd**command can affect the **ipv6 ospf bfd**command.
15.2(1)T	Use of the **ospfv3 bfd**command can affect the **ipv6 ospf bfd**command.

Usage Guidelines

Enter the **ipv6 ospf bfd** command to configure an OSPFv3 interface to use BFD for failure detection. If you have used the **bfd all-interfaces** command in router configuration mode to globally configure all OSPFv3 interfaces for an OSPFv3 process to use BFD, you can enter the **ipv6 ospf bfd** command in interface configuration mode with the **disable** keyword to disable BFD for a specific OSPFv3 interface.

Examples

In the following example, the interface associated with OSPFv3, Fast Ethernet interface 3/0, is configured for BFD:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# ipv6 ospf bfd
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
ospfv3 bfd	Enables BFD on an interface.

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf cost

To explicitly specify the cost of sending a packet on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ipv6 ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ipv6 ospf cost *interface-cost* | *dynamic* [**weight** {**throughput** *percent* | **resources** *percent* | **latency** *percent* | **L2-factor** *percent*] | [**hysteresis** | **threshold** *threshold-value*]]

no ipv6 ospf cost

Syntax Description

interface-cost	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.
dynamic	Default value on VMI interfaces.
weight	(Optional) Amount of impact a variable has on the dynamic cost.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The percent value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The percent value can be in the range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The percent value can be in the range from 0 to 100. The default value is 100.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The percent value can be in the range from 0 to 100. The default value is 100.
hysteresis	(Optional) Value used to dampen cost changes.
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64K, and the default threshold value is 10K.

Command Default

Default cost is based on the bandwidth.

Default cost on VMI interfaces is dynamic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(15)XF	The following keywords and arguments were added to support Virtual Multipoint Interfaces (VMI) and Mobile Adhoc Networking: • *dynamic* argument • **weight**, **resources** *percent* , **latency** *percent* , and **L2-factor** *percent* keywords and arguments.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.
15.2(1)T	Use of the **ospfv3 cost** command can affect the **ipv6 ospf cost** command.

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link-Default cost is 1785.
- 64-kbps serial link-Default cost is 1562.
- T1 (1.544-Mbps serial link)-Default cost is 64.
- E1 (2.048-Mbps serial link)-Default cost is 48.
- Ethernet-Default cost is 10.
- 16-Mbps Token Ring-Default cost is 6.
- FDDI-Default cost is 1.
- X25-Default cost is 5208.
- Asynchronous-Default cost is 10,000.
- ATM- Default cost is 1.The dynamic cost is calculated using the following formula:

  L2L3API

Where the metric calculations are:

S1 = ipv6 ospf dynamic weight throughput

S2 = ipv6 ospf dynamic weight resources

S3 = ipv6 ospf dynamic weight latency

S4 = ipv6 ospf dynamic weight L2 factor

OC = standard cost of a non-VMI route

Throughput = (current-data-rate)/(maximum-data-rate)

Router-dynamic cost= OC + (S1) + (S2) + (S3) + (S4)

For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold**threshold-value keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

Examples

The following example sets the interface cost value to 65:

```
ipv6 ospf cost 65
```

The following example sets the interface cost value for a VMI interface:

```
interface vmi 0
ipv6 ospf cost dynamic hysteresis threshold 30
ipv6 ospf cost dynamic weight throughput 75
ipv6 ospf cost dynamic weight resources 70
ipv6 ospf cost dynamic weight latency 80
ipv6 ospf cost dynamic weight L2-factor 10
```

Related Commands

Command	Description
interface vmi	Creates a virtual multipoint interface that can be configured and applied dynamically.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 cost	Explicitly specifies the cost of sending a packet on an interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First version 3 (OSPFv3) interface, use the **ip v6 ospf database-filter all out**command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ipv6 ospf database-filter all out
no ipv6 ospf database-filter all out

Syntax Description

This command has no arguments or keywords.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 database-filter**command can affect the **ipv6 ospf database-filter all out**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 database-filter**command can affect the **ipv6 ospf database-filter all out**command.
15.2(1)T	Use of the **ospfv3 database-filter**command can affect the **ipv6 ospf database-filter all out**command.

Usage Guidelines

This command performs the same function that the **neighbor database-filter**command performs on a neighbor basis.

Examples

The following example prevents flooding of OSPFv3 LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ipv6 ospf database-filter all out
```

Related Commands

ospfv3 database-filter	Filters outgoing LSAs to an OSPFv3 interface

router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

IPv6 Commands: ipv6 ospf de to ipv6 sp

ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **i pv6 ospf dead-interval**command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network.

Command Default

Four times the interval set by the **ipv6 ospf hello-interval** command

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 dead-interval**command can affect the **ipv6 ospf dead-interval**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 dead-interval**command can affect the **ipv6 ospf dead-interval**command.
15.2(1)T	Use of the **ospfv3 dead-interval**command can affect the **ipv6 ospf dead-interval**command.

Usage Guidelines

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

When the **ospfv3 dead-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 dead-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

Examples

The following example sets the Open Shortest Path First version 3 (OSPFv3) dead interval to 60 seconds:

```
interface ethernet 1
 ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
ipv6 ospf hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
ospfv3 dead-interval	Sets the time period for which hello packets must not be seen before neighbors declare the router down.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf demand-circuit

To configure Open Shortest Path First (OSPF) to treat the interface as an OSPFv3 demand circuit, use the **ip v6 ospf demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ipv6 ospf demand-circuit[**disable**] [**ignore**]
no ipv6 ospf demand-circuit

Syntax Description

disable	(Optional) Disables OSPFv3 from treating the interface as an OSPF v3demand circuit.
ignore	(Optional) Ignores requests from other routers to operate the link in demand-circuit mode.

Command Default

The circuit is not a demand circuit.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 demand-circuit**command can affect the **ipv6 ospf demand-circuit**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 demand-circuit**command can affect the **ipv6 ospf demand-circuit**command.
15.2(1)T	Use of the **ospfv3 demand-circuit**command can affect the **ipv6 ospf demand-circuit**command.
Cisco IOS XE Release 3.8S	This command was modified. The **ignore** keyword was added.

Usage Guidelines

When the **ospfv3 demand-circuit**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf demand-circuit**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example sets the configuration for an ISDN on-demand circuit:

```
interface BRI0
 ipv6 ospf 1 area 1
 ipv6 ospf demand-circuit
```

Related Commands

ospfv3 demand-circuit	Configures OSPFv3 to treat the interface as an OSPFv3 demand circuit.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf encryption

To specify the encryption type for an interface, use the **ipv6 ospf encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ipv6 ospf encryption {**ipsec spi** *spi* **esp** {*encryption-algorithm* [[*key-encryption-type*] *key*] | **null**} *authentication-algorithm* [{*key-encryption-type*}] *key* | **null**}
no ipv6 ospf encryption ipsec spi *spi*

Syntax Description

ipsec	Specifies IP Security (IPsec).
spi *spi*	Specifies the security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cbc**—Enables AES-CBC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null** —ESP with no encryption.
key-encryption-type	(Optional) One of two values can be entered: • **0** —The key is not encrypted. • **7** —The key is encrypted.
key	(Optional) Number used in the calculation of the message digest. The number is 32 hexadecimal digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow you to choose the size of the key.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5** —Enables message digest 5 (MD5) authentication. • **sha1** —Enables Secure Hash Algorithm 1 (SHA-1) authentication.
null	Overrides area encryption.

Command Default

Authentication and encryption are not configured on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(3)S	This command was modified. Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
Cisco IOS XE Release 3.4S	This command was modified. Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
15.2(1)T	This command was modified. Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When the **ipv6 ospf encryption** command is enabled, both authentication and encryption are enabled.

You need to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a device. This means that two IPsec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area encryption. If area encryption is not configured, then it is not necessary to configure the interface with the **ipv6 ospf encryption null** command.

Examples

The following example shows how to specify the encryption type for Ethernet interface 0/0. The IPsec SPI value is 1001, ESP is used with no encryption, and the authentication algorithm is SHA-1.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPFv3 area.
area encryption	Enables encryption for an OSPFv3 area.
area virtual-link authentication	Enables authentication for virtual links in an OSPFv3 area.
ipv6 ospf authentication	Specifies the authentication type for an interface.
ospfv3 encryption	Specifies the encryption type for an interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ip v6 ospf flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 ospf flood-reduction
no ipv6 ospf flood-reduction

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 flood-reduction**command can affect the **ipv6 ospf flood-reduction**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 flood-reduction**command can affect the **ipv6 ospf flood-reduction**command.
15.2(1)T	Use of the **ospfv3 flood-reduction**command can affect the **ipv6 ospf flood-reduction**command.

Usage Guidelines

When the **ospfv3 flood-reduction**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf flood-reduction**configuration if OSPFv3 was attached to the interface using the ipv6 ospf flood-reduction command.

All routers supporting the Open Shortest Path First version 3 (OSPFv3) demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example suppresses the flooding of unnecessary LSAs on serial interface 0:

```
interface serial 0
 ipv6 ospf flood-reduction
```

Related Commands

Command	Description
ospfv3 flood-reduction	Suppresses the unnecessary flooding of LSAs in stable topologies.
show ipv6 ospf interface	Displays OSPFv3-related interface information.
show ipv6 ospf neighbor	Displays OSPFv3-neighbor information on a per-interface basis.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ip v6 ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf hello-interval *seconds*
no ipv6 ospf hello-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Command Default

The default interval is 10 seconds when using Ethernet and 30 seconds when using nonbroadcast.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore**command.
15.2(1)T	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.

Usage Guidelines

When the **ospfv3 hello-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf hello-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

This value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
interface ethernet 1
 ipv6 ospf hello-interval 15
```

Related Commands

Command	Description
ipv6 ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router down.
ospfv3 hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.

ipv6 ospf mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the i**p v6 ospf mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore**command.
15.2(1)T	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.

Usage Guidelines

When the **ospfv3 mtu-ignore**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf mtu-ignore**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
interface serial 0/0
 ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
ospfv3 mtu-ignore	Disables OSPFv3 MTU mismatch detection on receiving DBD packets.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf name-lookup

To display Open Shortest Path First (OSPF) router IDs as Domain Naming System (DNS) names, use the **ipv6 ospf name-lookup** command in global configuration mode. To stop displaying OSPF router IDs as DNS names, use the **no** form of this command.

ipv6 ospf name-lookup
no ipv6 ospf name-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Examples

The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
ipv6 ospf name-lookup
```

ipv6 ospf neighbor

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **ip v6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]
no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Syntax Description

ipv6-address	Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
priority *number*	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified.The default is 0.
poll-interval *seconds*	(Optional) A number value that represents the poll interval time (in seconds). RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.
cost *number*	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the **ipv6 ospf cost**command.
database-filter all out	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

Command Default

No configuration is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be a link-local address of the neighbor.

If a neighboring router has become inactive (hello packets have not been seen for the Router Dead Interval period), hello packets may need to be sent to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

The **priority** keyword does not apply to point-to-multipoint interfaces. For point-to-multipoint interfaces, the **cost** keyword and the number argument are the only options that are applicable. The **cost** keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

Examples

The following example configures an OSPF neighboring router:

```
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

ipv6 ospf network

To configure the Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for a given medium, use the **i pv6 ospf network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ipv6 ospf network {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}
no ipv6 ospf network

Syntax Description

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint non-broadcast	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to be nonbroadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

Default depends on the network type.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)XF	The **point-to-multipint** keyword was added to support the Virtual Multipoint Interfaces (VMI) and Mobile Adhoc Networking.
12.4(15)T	This command was integrated into Cisco IOS 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 network**command can affect the **ipv6 ospf network**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 network**command can affect the **ipv6 ospf network**command.
15.2(1)T	Use of the **ospfv3 network**command can affect the **ipv6 ospf network**command.

Usage Guidelines

When the ospfv3 networkcommand is configured with the *process-id* argument, it overwrites the ipv6 ospf networkconfiguration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

NBMA Networks

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure NBMA networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service [SMDS]) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, the assumption is not true for other configurations, such as for a partially meshed network. In these cases, you can configure the OSPFv3 network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

Point-to-Multipoint Networks

OSPFv3 for IPv6 has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

OSPFv3 Network as Broadcast Network Example

The following example sets your OSPFv3 network as a broadcast network:

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf network broadcast
 encapsulation frame-relay
```

OSPFv3 Point-to-Multipoint Network with Broadcast Example

The following example illustrates a point-to-multipoint network with broadcast:

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 ipv6 ospf cost 100
 ipv6 ospf network point-to-multipoint
 frame-relay map ipv6 2001:0DB1::A8BB:CCFF:FE00:C01 broadcast
 frame-relay map ipv6 2001:0DB1B:CCFF:FE00:C02 broadcast
 frame-relay local-dlci 200
 ipv6 ospf neighbor 2001:0DB1B:CCFF:FE00:C01
 ipv6 ospf neighbor2001:0DB1B:CCFF:FE00:C02
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 network	Configures an OSPFv3 network type to a type other than the default for a given medium.
x25 map	Sets up the LAN protocols-to-remote host mapping.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf priority

To set the router priority, which helps determine the designated router for this network, use the **i pv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *number-value*
no ipv6 ospf priority *number-value*

Syntax Description

number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

The router priority is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 priority**command can affect the **ipv6 ospf priority**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 priority**command can affect the **ipv6 ospf priority**command.
15.2(1)T	Use of the **ospfv3 priority**command can affect the **ipv6 ospf priority**command.

Usage Guidelines

When the **ospfv3 priority**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf priority**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First version 3 (OSPFv3) for nonbroadcast networks using the **ipv6 ospf neighbor** command.

Examples

The following example sets the router priority value to 4:

```
interface ethernet 0
 ipv6 ospf priority 4
```

Related Commands

Command	Description
ipv6 ospf network	Configures the OSPFv3 network type to a type other than the default for a given medium.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 priority	Sets the router priority, which helps determine the designated router for this network.

ipv6 ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First version 3 (OSPFv3) interface, use the **ip v6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *seconds*
no ipv6 ospf retransmit-interval

Syntax Description

seconds	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 retransmit-interval**command can affect the **ipv6 ospf retransmit-interval**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 retransmit-interval**command can affect the **ipv6 ospf retransmit-interval**command.
15.2(1)T	Use of the **ospfv3 retransmit-interval**command can affect the **ipv6 ospf retransmit-interval**command.

Usage Guidelines

When the **ospfv3 retransmit-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf retransmit-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
interface ethernet 2
 ipv6 ospf retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 retransmit-interval	Specifies the time between LSA retransmissions for adjacencies belonging to the interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf transmit-delay

To set the estimated time required to send a link-state update packet on the Open Shortest Path First version 3 (OSPFv3) interface, use the **i p ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *seconds*
no ipv6 ospf transmit-delay

Syntax Description

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

The default is 1 second.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 transmit-delay**command can affect the **ipv6 ospf transmit-delay**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 transmit-delay** command can affect the **ipv6 ospf transmit-delay**command.
15.2(1)T	Use of the **ospfv3 transmit-delay**command can affect the **ipv6 ospf transmit-delay**command.

Usage Guidelines

When the **ospfv3 transmit-delay**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf transmit-delay**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
interface ethernet 0
 ipv6 ospf transmit-delay 3
```

Related Commands

Command	Description
ospfv3 transmit-delay	Sets the estimated time required to send a link-state update packet on the interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 pim

To reenable IPv6 Protocol Independent Multicast (PIM) on a specified interface, use the **ipv6 pim**command in interface configuration mode. To disable PIM on a specified interface, use the **no** form of the command.

ipv6 pim
no ipv6 pim

Syntax Description

This command has no arguments or keywords.

Command Default

PIM is automatically enabled on every interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface. When PIM is disabled on an interface, it does not react to any host membership notifications from the Multicast Listener Discovery (MLD) protocol.

Examples

The following example turns off PIM on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 pim
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the **ipv6 pim accept-register**command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}
no ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
list *access-list*	Defines the access list name.
route-map *map-name*	Defines the route map.

Command Default

All sources are accepted at the RP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 pim accept-register**command to configure a named access list or route map with match attributes. When the permit conditions as defined by the *access-list* and *map-name* arguments are met, the register message is accepted. Otherwise, the register message is not accepted, and an immediate register-stop message is returned to the encapsulating designated router.

Examples

The following example shows how to filter on all sources that do not have a local multicast Border Gateway Protocol (BGP) prefix:

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
 match as-path 101
ip as-path access-list 101 permit
```

ipv6 pim allow-rp

To enable the PIM Allow RP feature for all IP multicast-enabled interfaces in an IPv6 device, use the **ip pim allow-rp** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim allow-rp [{**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]}]
no ipv6 pim allow-rp

Syntax Description

group-list	(Optional) Identifies an access control list (ACL) of allowed group ranges for PIM Allow RP.
rp-list	(Optional) Specifies an ACL for allowed rendezvous-point (RP) addresses for PIM Allow RP.
access-list	(Optional) Unique number or name of a standard ACL.

Command Default

PIM Allow RP is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to enable the receiving device in an IP multicast network to accept a (*, G) Join from an unexpected (different) RP address.

Before enabling PIM Allow RP, you must first use the **ipv6 pim rp-address** command to define an RP.

Examples

NEED CONFIG EXAMPLE HERE

Related Commands

Command	Description
ipv6 pim rp-address	Statically configures the address of a PIM RP for multicast groups.

ipv6 pim anycast-RP

To configure the address of the Protocol-Independent Multicast (PIM) rendezvous point (RP) for an anycast group range, use the **ipv6 pim anycast-RP** command in global configuration mode. To remove an RP address for an anycast group range, use the **no** form of this command.

ipv6 pim anycast-RP {*rp-address* *peer-address*}
no ipv6 pim anycast-RP

Syntax Description

anycast-rp-address	Anycast RP set for the RP assigned to the group range. This is the address that first-hop and last-hop PIM routers use to register and join.
peer-address	The address to which register messages copies are sent. This address is any address assigned to the RP router, not including the address assigned using the *anycast-rp-address* variable.

Command Default

No PIM RP address is configured for an anycast group range.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(3)T	This command was integrated into Cisco IOS XE Release 15.2(3)T.
15.1(1)SY	This command was integrated into Cisco IOS XE Release 15.1(1)SY.

Usage Guidelines

The anycast RP feature is useful when interdomain connection is not required. Use this command to configure the address of the PIM RP for an anycast group range.

Examples

```
Router# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::3:3
```

Related Commands

Command	Description
show ipv6 pim anycast-RP	Verifies IPv6 PIM RP anycast configuration.

ipv6 pim bsr border

To configure a border for all bootstrap message (BSMs) of any scope on a specified interface, use the **ipv6 pim bsr border**command in interface configuration mode. To remove the border, use the **no** form of this command.

ipv6 pim bsr border
no ipv6 pim bsr border

Syntax Description

This command has no argument or keywords.

Command Default

No border is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 pim bsr border** command is used to configure a border to all global and scoped BSMs. The command filters incoming or outgoing BSMs, preventing the BSMs from being forwarded or accepted on the interface on which the **ipv6 pim bsr border** command is configured.

Examples

The following example configures a BSR border on Ethernet interface 1/0:

```
Router(config)# interface Ethernet1/0
 Router(config-if)# ipv6 pim bsr border
 Router(config-if)# end
Router# show running-config interface e1/0
 Building configuration...
 Current configuration :206 bytes
 !
 interface Ethernet1/0
 ipv6 address 2:2:2::2/64
 ipv6 enable
 ipv6 rip test enable
```

```
ipv6 pim bsr border
no cdp enable
end
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router as a candidate BSR.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate bsr

To configure a device to be a candidate bootstrap device (BSR), use the **ipv6 pim bsr candidate bsr**command in global configuration mode. To remove this device as a candidate BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope**] [**accept-rp-candidate** *acl-name*]
no ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope**] [**accept-rp-candidate** *acl-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the device to be configured as a candidate BSR. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
hash-mask-length	(Optional) The length (in bits) of the mask to use in the BSR hash function. The default value is 126.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192. The BSR with the larger priority is preferred. If the priority values are the same, the device with the larger IPv6 address is the BSR. The default value is 0.
scope	(Optional) BSR will originate bootstrap messages (BSMs), including the group range associated with the scope, and accept candidate RP (C-RP) announcements only if they are for groups that belong to the given scope.
accept-rp-candidate *acl-name*	(Optional) BSR C-RP advertisements will be filtered at the BSR using the named access list (*acl-name*) for the RP candidates.

Command Default

Device is not enabled as a BSR.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	The **scope** keyword and *scope-value* argument were added.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(1)S	This command was modified. The **accept-rp-candidate** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to configure a device as a candidate BSR; however, the device becomes a candidate only if the address belongs to a PIM-enabled interface. When a device is configured, it will participate in BSR election. If elected BSR, this device will periodically originate BSR messages advertising the group-to-RP mappings it has learned through candidate-RP-advertisement messages.

If the **scope** keyword is enabled, the BSR will originate BSMs, including the group range associated with the scope, and accept C-RP announcements only if they are for groups that belong to the given scope. If no scope is configured, all scopes are used.

The **accept-rp-candidate** *acl-name* keyword and argument will restrict the C-RP candidates accepted. If the **accept-rp-candidate** keyword is not configured, BSR C-RP advertisements at the BSR are not filtered.

Examples

The following example configures the device with the IPv6 address 2001:0DB8:3000:3000::42 as the candidate BSR, with a hash mask length of 124 and a priority of 10:

```
ipv6 pim bsr candidate bsr 2001:0DB8:3000:3000::42 124 priority 10
```

The following example will restrict the C-RP advertisements accepted. The ACL, crp, is used to filter the advertisements.

```
ipv6 pim bsr candidate bsr 194::1:1:2 priority 150 accept-rp-candidate crp
acl crp with
permit ipv6 host 192::1:1:1 any log
deny ipv6 any any log
```

Related Commands

Command	Description
ipv6 pim bsr border	Configures a border for all bootstrap message BSMs of any scope.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate rp

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap device (BSR), use the **ipv6 pim bsr candidate rp** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
no ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the device to be advertised as the candidate RP (C-RP). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-list	(Optional) List of group prefixes. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
access-list-name	(Optional) Name of the IPv6 access list containing group prefixes that will be advertised in association with the RP address. Names cannot contain a space or quotation mark, or begin with a numeral. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If the access list contains any group address ranges that overlap the assigned SSM group address range (FF3x::/96), a warning message is displayed, and the overlapping address ranges are ignored.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192 that specifies the priority. The RP with the higher priority is preferred. If the priority values are the same, the device with the higher IPv6 address is the RP. The default value is 192.
interval	(Optional) Configures the C-RP advertisement interval.
seconds	(Optional) Advertisement interval in number of seconds.
scope	(Optional) Device advertises itself as the C-RP only to the BSR for the specified scope.
scope-value	(Optional) Integer from 3 through 15 that specifies the scope.
bidir	(Optional) Device advertises itself as the C-RP for the **group-list** *access-list-name* in the bidirectional range.

Command Default

Device is not enabled as a candidate RP. If no scope is configured, all scopes are advertised.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	The **scope** and **bidir** keywords were added. The *scope-value* argument was added.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use this command to send PIM RP advertisements to the BSR. The PIM RP advertisement becomes a candidate only if the address belongs to a PIM-enabled interface.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority***priority-value* keyword and argument are specified, then the device will announce itself to be a candidate RP with the specified priority.

If the **scope** keyword is used, the device advertises itself as the C-RP only to the BSR for the specified scope. If the **group-list**keyword is specified along with the scope, then only prefixes in the *access-list-name* argument with the same scope as the scope configured will be advertised. If no scope is configured, all scopes are advertised.

Examples

The following example configures the device with the IPv6 address 2001:0DB8:3000:3000::42 to be advertised as the candidate RP, with a priority of 0:

```
Device(config)# ipv6 pim bsr candidate rp 2001:0DB8:3000:3000::42 priority 0
```

The following example configures the device with the IPv6 address 2001:0DB8:1:1:1 as the candidate RP for scope 6 for the group ranges specified in the access list named list1:

```
Device(config)# ipv6 pim bsr candidate rp 2001:0DB8:1:1:1 group-list list1 scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a device as a candidate BSR.
ipv6 pim bsr border	Configures a border for all BSMs of any scope.

ipv6 pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ipv6 pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim dr-priority *value*
no ipv6 pim dr-priority

Syntax Description

value	An integer value to represent DR priority. Value range is from 0 to 4294967294. The default value is 1.

Command Default

Default value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **ipv6 pim dr-priority** command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IPv6 address on the interface becomes the DR.

If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address becomes the DR.

Examples

The following example configures the router to use DR priority 3:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim dr-priority 3
```

Related Commands

Command	Description
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.

ipv6 pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ipv6 pim hello-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ipv6 pim hello-interval *seconds*
no ipv6 pim hello-interval *seconds*

Syntax Description

seconds	Interval, in seconds, at which PIM hello messages are sent.

Command Default

Hello messages are sent at 30-second intervals with small random jitter.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Periodic hello messages are sent out at 30-second intervals with a small jitter. The **ipv6 pim hello-interval**command allows users to set a periodic interval.

Examples

The following example sets the PIM hello message interval to 45 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim hello-interval 45
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 pim dr-priority	Configures the DR priority on a PIM router.
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

ipv6 pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ipv6 pim join-prune-interval**command in interface configuration mode. To return to the default value, use the **no** form of the command.

ipv6 pim join-prune-interval *seconds*
no ipv6 pim join-prune-interval *seconds*

Syntax Description

seconds	The join and prune announcement intervals, in number of seconds. The default value is 60 seconds.

Command Default

The default is 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Periodic join and prune announcements are sent out at 60-second intervals. The **ipv6 pim join-prune-interval** commandallows users to set a periodic interval.

Examples

The following example sets the join and prune announcement intervals to 75 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim join-prune-interval 75
```

ipv6 pim neighbor-filter list

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the **ipv6 pim neighbor-filter** command in the global configuration mode. To return to the router default, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*
no ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of an IPv6 access list that denies PIM hello packets from a source.

Command Default

PIM neighbor messages are not filtered.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 pim neighbor-filter list**command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

Examples

The following example causes PIM to ignore all hello messages from IPv6 address FE80::A8BB:CCFF:FE03:7200:

```
Router(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Router(config)# ipv6 access-list nbr_filter_acl
Router(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Router(config-ipv6-acl)# permit any any
```

ipv6 pim passive

To enable the Protocol Independent Multicast (PIM) passive feature on a specific interface, use the **ipv6 pim passive**command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 pim passive
no ipv6 pim passive

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **ipv6 pim passive**command to configure IPv6 PIM passive mode on an interface.

A PIM passive interface does not send or receive any PIM control messages. However, a PIM passive interface acts as designated router (DR) and designated forwarder (DF)-election winner, and it can accept and forward multicast data.

Examples

The following example configures IPv6 PIM passive mode on an interface:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# ipv6 pim passive
```

Related Commands

Command	Description
ipv6 multicast pim-passive-enable	Enables the PIM passive feature on an IPv6 router.

ipv6 pim rp embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded**command in global configuration mode. To disable embedded RP support, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp embedded**
no ipv6 pim [**vrf** *vrf-name*] **rp embedded**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Embedded RP support is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support.

The **ipv6 pim rp embedded**command applies only to the embedded RP group ranges ff7X::/16 and fffX::/16. When the router is enabled, it parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples

The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp embedded
```

ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
no ipv6 pim rp-address *ipv6-address* [*group-access-list*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of a router to be a PIM RP. The *ipv6-address*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-access-list	(Optional) Name of an access list that defines for which multicast groups the RP should be used. If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range (FF3x::/96), a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges. To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address. Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7).
bidir	(Optional) Indicates that the group range will be used for bidirectional shared-tree forwarding; otherwise, it will be used for sparse-mode forwarding. A single IPv6 address can be configured to be RP only for either bidirectional or sparse-mode group ranges. A single group-range list can be configured to operate either in bidirectional or sparse mode.

Command Default

No PIM RPs are preconfigured. Embedded RP support is enabled by default when IPv6 PIM is enabled (where embedded RP support is provided). Multicast groups operate in PIM sparse mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	Embedded RP support was added.
12.3(7)T	The **bidir** keyword was added to Cisco IOS Release 12.3(7)T.

Release	Modification
12.2(25)S	The **bidir** keyword was added to Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

When PIM is configured in sparse mode, you must choose one or more routers to operate as the RP. An RP is a single common root of a shared distribution tree and is statically configured on each router.

Where embedded RP support is available, only the RP needs to be statically configured as the RP for the embedded RP ranges. No additional configuration is needed on other IPv6 PIM routers. The other routers will discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional *group-access-list* argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96. If the *group-access-list* argument is specified, the IPv6 address is the RP address for the group range specified in the *group-access-list* argument.

You can configure Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

Examples

The following example shows how to set the PIM RP address to 2001::10:10 for all multicast groups:

```
Router(config)# ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any ff04::/64
Router(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
Router(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
```

```
Router(config)# ipv6 access-list embd-ranges
Router(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

The following example shows how to enable the address 100::1 as the bidirectional RP for the entries multicast range FF::/8:

```
ipv6 pim rp-address 100::1 bidir
```

In the following example, the IPv6 address 200::1 is enabled as the bidirectional RP for the ranges permitted by the access list named bidir-grps. The ranges permitted by this list are ff05::/16 and ff06::/16.

```
Router(config)# ipv6 access-list bidir-grps
Router(config-ipv6-acl)# permit ipv6 any ff05::/16
Router(config-ipv6-acl)# permit ipv6 any ff06::/16
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

ipv6 pim spt-threshold infinity

To configure when a Protocol Independent Multicast (PIM) leaf router joins the shortest path tree (SPT) for the specified groups, use the **ipv6 pim spt-threshold infinity**command in global configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
no ipv6 pim spt-threshold infinity

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-list *access-list-name*	(Optional) Indicates to which groups the threshold applies. Must be a standard IPv6 access list name. If the value is omitted, the threshold applies to all groups.

Command Default

When this command is not used, the PIM leaf router joins the SPT immediately after the first packet arrives from a new source. Once the router has joined the SPT, configuring the **ipv6 pim spt-threshold infinity**command will not cause it to switch to the shared tree.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

Using the **ipv6 pim spt-threshold infinity**command enables all sources for the specified groups to use the shared tree. The **group-list** keyword indicates to which groups the SPT threshold applies.

The *access-list-name*argument refers to an IPv6 access list. When the *access-list-name*argument is specified with a value of 0, or the **group-list** keyword is not used, the SPT threshold applies to all groups. The default setting (that is, when this command is not enabled) is to join the SPT immediately after the first packet arrives from a new source.

Examples

The following example configures a PIM last-hop router to stay on the shared tree and not switch to the SPT for the group range ff04::/64.:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any FF04::/64
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

ipv6 policy route-map

To configure IPv6 policy-based routing (PBR) on an interface, use the **ipv6 policy route-map** command in interface configuration mode. To disable IPv6 PBR on an interface, use the **no** form of this command.

ipv6 policy route-map *route-map-name*
no ipv6 policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to be used for PBR. The name must match the *map-tag* value specified by a **route-map** command.

Command Default

Policy-based routing does not occur on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can enable PBR if you want your packets to take a route other than the obvious shortest path.

The **ipv6 policy route-map** command identifies a route map to be used for policy-based routing. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which PBR is allowed for the interface. The **set** commands specify set actions, which are the PBR actions to be performed if the criteria enforced by the **match** commands are met. The **no ipv6 policy route-map** command deletes the pointer to the route map.

Policy-based routing can be performed on any match criteria that can be defined in an IPv6 access list.

Examples

In the following example, a route map named pbr-dest-1 is created and configured, specifying the packet match criteria and the desired policy-route action. Then, PBR is enabled on the interface Ethernet0/0.

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8::1
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface Ethernet0/0
interface Ethernet0/0
  ipv6 policy-route-map pbr-dest-1
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies the route map to be used for local IPv6 PBR.
match ipv6 address	Specifies an IPv6 access list to be used to match IPv6 packets for PBR.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Specifies the default interface to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 port-map

To establish port-to-application mapping (PAM) for the system, use the **ipv6 port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ipv6 port-map *application* **port** *port-num* [**list** *acl-name*]
no ipv6 port-map *application* **port** *port-num* [**list** *acl-name*]

Syntax Description

application	Specifies the predefined application that requires port mapping.
port *port-num*	Specifies a port number. The range is from 1 to 65535.
list *acl-name*	(Optional) Specifies the name of the IPv6 access list (ACL) associated with the port mapping.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **ipv6 port-map** command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

The table below lists the default system-defined services and applications in the PAM table.

Table 6: System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol (SMTP)
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override the system-defined entries for a specific host or subnet using the **list** keyword in the **ipv6 port-map** command.

User-Defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ipv6 port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ipv6 port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ipv6 port-map** command to associate another service or application with the specific port.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** keyword for the **ipv6 port-map** command to specify an ACL for a host or subnet that uses PAM.

Note If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following user-defined port-mapping configuration map port 8080 to the HTTP application:

```
ipv6 port-map http port 8080
```

Host-specific port-mapping configuration maps port 2121 to the FTP application from a particular set of host. First, the user needs to create a permit IPv6 access list for the allowed host(s). In the following example, packets from the hosts in the 2001:0DB8:1:7 subset destined for port 2121 will be mapped to the FTP application:

```
Router(config)# ipv6 access-list ftp-host
Router(config-ipv6-acl)# permit 2001:0DB8:1:7::/64 any
```

The port-map configuration is then configured as follows:

```
Router(config)# ipv6 port-map ftp port 2121 list ftp-host
```

Related Commands

Command	Description
show ipv6 port-map	Displays IPv6 port-mapping information.

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

ipv6 prefix-list *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix/prefix-length* | **permit** *ipv6-prefix/prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]
no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. • Cannot be the same name as an existing access list. • Cannot be the name "detail" or "summary" because they are keywords in the **show ipv6 prefix-list** command.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that matches the condition.
permit	Permits networks that matches the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. 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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix/prefix-length* arguments. It is the lowest value of a range of the *length* (the "from" portion of the length range).
le *le-value*	(Optional) Specifies a prefix length less than or equal to the *ipv6-prefix /prefix-length* arguments. It is the highest value of a range of the *length* (the "to" portion of the length range).

Command Default

No prefix list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.

Release	Modification
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

To suppress networks from being advertised in updates, use the **distribute-list out** command.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you may want to put the most common permits or denies near the top of the list, using the *seq-number* argument.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual *ipv6-prefix/prefix-length* argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

- The candidate prefix must match the specified prefix list and prefix length entry.
- The value of the optional **le** keyword specifies the range of allowed prefix lengths from the *prefix-length* argument up to, and including, the value of the **le** keyword.
- The value of the optional **ge** keyword specifies the range of allowed prefix lengths from the value of the **ge** keyword up to, and including, 128.

Note The first condition must match before the other conditions take effect.

An exact match is assumed when the **ge** or **le** keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The *prefix-length* value must be less than the **ge** value. The **ge** value must be less than, or equal to, the **le** value. The **le** value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have any permit and deny condition statements, has an implicit deny any any statement as its last match condition.

Examples

The following example denies all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix 2002::/16:

```
Router(config)# ipv6 prefix-list abc permit 2002::/16
```

The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64.

```
Router(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64.

```
Router(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

The following example permits mask lengths from 32 to 64 bits in all address space.

```
Router(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example denies mask lengths greater than 32 bits in all address space.

```
Router(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
Router(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the IPv6 prefix list entries.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

ipv6 redirects

To enable the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received, use the **ipv6 redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ipv6 redirects
no ipv6 redirects

Syntax Description

This command has no arguments or keywords.

Command Default

The sending of ICMP IPv6 redirect messages is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval** command.

Examples

The following example disables the sending of ICMP IPv6 redirect messages on Ethernet interface 0 and reenables the messages on Ethernet interface 1:

```
Router(config)# interface ethernet 0
Router(config-if)# no ipv6 redirects
Router(config)# interface ethernet 1
Router(config-if)# ipv6 redirects
```

To verify whether the sending of IPv6 redirect messages is enabled or disabled on an interface, enter the **show ipv6 interface** command:

```
Router# show ipv6 interface
Ethernet0 is up, line protocol is up
```

```
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2000::1, subnet is 2000::/64
    3000::1, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are disabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised 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.
Ethernet1 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::2
  Global unicast address(es):
    2000::2, subnet is 2000::/64
    3000::3, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is disabled, number of DAD attempts: 0
  ND reachable time is 30000 milliseconds
  ND advertised 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 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 rip default-information

To originate a de fault IPv6 route into the Routing Information Protocol (RIP), use the **ipv6 rip default-information**command in interface configuration mode. To remove the default IPv6 RIP route, use the **no** form of this command.

ipv6 rip *name* **default-information** {**only** | **originate**} [**metric** *metric-value*]
no ipv6 rip *name* **default-information**

Syntax Description

name	Name of the IPv6 RIP routing process.
only	Advertises the IPv6 default route (::/0) only. Suppresses the advertisement of all other routes.
originate	Advertises the IPv6 default route (::/0). The advertisement of other routes is unaffected.
metric *metric-value*	(Optional) Associates a metric with the default route. The *metric-value* range is from 1 through 15.

Command Default

Metric value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(14)T	The **metric** keyword and *metric-value* argument were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 rip default-information**command is similar to the **default-information originate** (RIP)command, except that it is IPv6-specific.

Originating a default IPv6 route into RIP also forces the advertisement of the route in router updates sent on the interface. The advertisement of the route occurs regardless of whether the route is present in the IPv6 routing table.

The **metric***metric-value* keyword and argument allow more flexibility in topologies with multiple RIP routers on a LAN. For example, a user may want to configure one of many routers on a LAN as the preferred default router, so that all default route traffic will transit this router. This function can be achieved by configuring the preferred router to advertise a default route with a lower metric than the other routers on the network.

Note To avoid routing loops after the IPv6 default route (::/0) is originated into a specified RIP routing process, the routing process ignores all default route information received in subsequent IPv6 RIP update messages.

Examples

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises only the default route in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information only
```

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises the default route with all other routes in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information originate
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip enable

To enable an IPv6 Routing Information Pr otocol (RIP) routing process on an interface, use the **ipv6 rip enable**command in interface configuration mode. To disable an IPv6 RIP routing process on an interface, use the **no** form of this command.

ipv6 rip *name* **enable**
no ipv6 rip *name*

Syntax Description

name	Name of the IPv6 RIP routing process.

Command Default

An IPv6 RIP routing process is not defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 rip enable** interface configuration command is used to enable IPv6 RIP explicitly on required interfaces. In IPv4, the **network***network-number* router configuration command is used to implicitly specify the interfaces on which to run IPv4 RIP.

Examples

The following example enables the IPv6 RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco enable
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip metric-offset

To set the IPv6 Routing Information Protocol (RIP) metric for an interface, use the **ipv6 rip metric-offset**command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

ipv6 rip *word* **metric-offset** *value*
no ipv6 rip *word* **metric-offset**

Syntax Description

word	Name of the IPv6 RIP routing process.
value	Value added to the metric of an IPv6 RIP route received in a report message. A number from 1 to 16.

Command Default

The default metric value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When an IPv6 RIP route is received, the interface metric value set by the **ipv6 rip metric-offset**command is added before the route is inserted into the routing table. Therefore, increasing the IPv6 RIP metric value of an interface increases the metric value of IPv6 RIP routes received over the interface.

Use the **ipv6 rip metric-offset** command to influence which routes are used, as you prefer. The IPv6 RIP metric is in hop count.

Examples

The following example configures a metric increment of 10 for the RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco metric-offset 10
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip summary-address

To configure IPv6 Routing Information Protocol (RIP) to advertise summarized IPv6 addresses on an interface and to specify the IPv6 prefix that identifies the routes to be summarized, use the **ipv6 rip summary-address**command in interface configuration mode. To stop the advertising of the summarized IPv6 addresses, use the **no** form of this command.

ipv6 rip *word* **summary-address** *ipv6-prefix/prefix-length*
no ipv6 rip *word* **summary-address**

Syntax Description

word	Name of the IPv6 RIP routing process.
ipv6-prefix	Specifies an IPv6 network number as the summary 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.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **ipv6 rip summary-address**command is similar to the **ip summary-address rip**command, except that it is IPv6-specific.

Use the **ipv6 rip summary-address**command to force IPv6 RIP to advertise specific networks on specific interfaces (assuming that routes to those networks exist).

If the first bits of the prefix length for a route match the value specified for the ipv6-prefixargument, the prefix specified in the ipv6-prefixargument is advertised instead of the route. As a result, multiple routes can be replaced by a single route whose metric is the lowest metric of the multiple routes.

Examples

In the following example, the IPv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 that is assigned to Ethernet interface 0/0 with an IPv6 prefix length of 64 bits is summarized as IPv6 prefix 2001:0DB8::/35 for the IPv6 RIP routing process named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 /64
Router(config-if)# ipv6 rip cisco summary-address 2001:0DB8::/35
```

Note A route advertisement that is suppressed as a result of split horizon is not considered by RIP when RIP is deciding whether to advertise a summary route.

Related Commands

Command	Description
poison-reverse (IPv6 RIP)	Configures the poison reverse processing of IPv6 RIP router updates.
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip vrf-mode enable

To enable VRF-aware support for IPv6 Routing Information Protocol (RIP), use the **ipv6 rip vrf-mode enable** command in global configuration mode. To disable VRF-aware support for IPv6 RIP, use the **no** form of this command.

ipv6 rip vrf-mode enable
no ipv6 rip vrf-mode enable

Syntax Description

This command has no arguments or keywords.

Command Default

VRF-aware support is not enabled in IPv6 RIP.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
15.3(2)S	This command was integrated into Cisco IOS Release 15.3(2)S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

When VRF-aware support is enabled in IPv6 RIP, you can configure only one RIP instance at a given time. More than one RIP instance is not allowed.

The following example shows how to enable VRF-aware support for IPv6 RIP routing.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 rip vrf-mode enable
Device(config)# end
```

Related Commands

Command	Description
clear ipv6 rip	Deletes routes from the IPv6 RIP routing table.
debug ipv6 rip	Displays debug messages for IPv6 RIP routing transactions.
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 route

To establish static IPv6 routes, use the **ipv6 route**command in global configuration mode. To remove a previously configured static route, use the **no** form of this command.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-type interface-number* [*i* **pv6-address**]} [**nexthop-vrf** [{*vrf-name1* | **default**}]] [*administrative-distance*] [{*administrative-multicast-distance* | **unicast** | **multicast**}] [*next-hop-address*] [**tag** *tag*] [**name** *name*]
no ipv6 route [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-type interface-number* [*i* **pv6-address**]} [**nexthop-vrf** [{*vrf-name1* | **default**}]] [*administrative-distance*] [{*administrative-multicast-distance* | **unicast** | **multicast**}] [*next-hop-address*] [**tag** *tag*] [**name** *route-name*]

Syntax Description

ipv6-prefix	The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
vrf	(Optional) Specifies all virtual private network (VPN) routing/forwarding instance (VRF) tables or a specific VRF table for IPv4 or IPv6 address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. When an interface type and interface number are specified, you can optionally specify the IPv6 address of the next hop to which packets are output. **Note** You must specify an interface type and an interface number when using a link-local address as the next hop (the link-local next hop must also be an adjacent device). 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 about supported interface types, use the question mark (?) online help function. You can use the *interface-type* argument to direct static routes out point-to-point interfaces (such as serial or tunnel interfaces) and broadcast interfaces (such as Ethernet interfaces). When using the *interface-type* argument with point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. When using the *interface-type* argument with broadcast interfaces, you should always specify the IPv6 address of the next hop or ensure that the specified prefix is assigned to the link. A link-local address should be specified as the next hop for broadcast interfaces.
interface-number	Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function.

nexthop-vrf	(Optional) Indicator that the next hop is a VRF.
vrf-name1	(Optional) Name of the next-hop VRF.
default	(Optional) Indicator that the next hop is the default.
administrative-distance	(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes.
administrative-multicast-distance	(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF).
unicast	(Optional) Specifies a route that must not be used in multicast RPF selection.
multicast	(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB).
next-hop-address	(Optional) Address of the next hop that can be used to reach the specified network.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.
name *route-name*	(Optional) Specifies a name for the route.

Command Default

No static routes are established.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The optional *ipv6-address* argument was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(26)S	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance*argument were added.
12.3(4)T	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance*argument were added.
12.2(25)S	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance*argument were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The optional **vrf** and **nexthop-vrf** keywords, and *vrf-name* and *next-hop-address* arguments were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
15.0	The **name** *name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **ipv6 route** command to implement static multicast routes in IPv6. For a static multicast route, the IPv6 address of the next-hop device must be provided. The *administrative-multicast-distance* argument determines the distance that will be used when selecting this route for RPF. When the **unicast** keyword is used, this route will not be used in multicast RPF selection.

When the **ipv6 route** command is used with the **multicast** keyword, the route will not be populated in the unicast RIB. When the optional *administrative-multicast-distance* argument is not specified, the multicast RPF administrative distance defaults to the same value as that determined by the *administrative-distance* argument.

Examples

The following example shows a static route that applies to unicast routing only:

```
ipv6 route 2001::/64 5::5 100 unicast
```

The following example shows a static route used only for multicast RPF selection:

```
ipv6 route 2001::/64 7::7 100 multicast
```

The following example shows a static route used for both unicast routing and multicast RPF selection:

```
ipv6 route 2001::/64 6::6 100
```

The following example shows a static route used for both unicast routing and multicast RPF selection, but with different administrative distances:

```
ipv6 route 10::/64 7::7 100 200
```

The following example configures a static route for use in VPN for IPv6:

```
ipv6 route vrf red 4004::/64 pos 1/0
```

The following example configures a static default route within a VRF. Use of the **global** keyword in this static route provides access to the Internet:

```
ipv6 route vrf red ::0/0 7007::1 global
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 rpf	Displays RPF information for a given unicast host address and prefix.

ipv6 route priority high

To assign a high-priority tag to an integrated Intermediate System-to-Intermediate System (IS-IS) IPv6 prefix to be used for controlling redistribution via route maps, use the **ipv6 route priority high** command in address family configuration mode. To remove the IPv6 prefix priority, use the **no** form of this command.

ipv6 route priority high tag *tag-value*
no ipv6 route priority high tag

Syntax Description

tag *tag-value*	Assigns a tag value that can be used as a match value for controlling redistribution via route maps. The range is from 1 to 4294967295.

Command Default

No priority is assigned to IS-IS IPv6 prefixes.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Examples

In the following example, a high-priority tag of 100 is assigned:

```
Device# configure terminal
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# ipv6 route priority high tag 100
```

Related Commands

Command	Description
isis ipv6 tag	Configures an administrative tag value that will be associated with an IPv6 address prefix and applied to an IS-IS LSP.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays additional information about the IS-IS database.
summary-prefix (IPv6 IS-IS)	Creates aggregate IPv6 prefixes for IS-IS.

ipv6 route static bfd

To specify static route Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors, use the **ipv6 route static bfd** command in global configuration mode. To remove a static route BFDv6 neighbor, use the **no** form of this command.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]
no ipv6 route static bfd

Syntax Description

vrf *vrf-name*	(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.
interface-type interface-number	Interface type and number.
ipv6-address	IPv6 address of the neighbor.
unassociated	(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Command Default

No static route BFDv6 neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **ipv6 route static bfd** command to specify static route neighbors. All of the static routes that have the same interface and gateway specified in the configuration share the same BFDv6 session for reachability notification. BFDv6 requires that BFDv6 sessions are initiated on both endpoint routers. Therefore, this command must be configured on each endpoint router. An IPv6 static BFDv6 neighbor must be fully specified (with the interface and the neighbor address) and must be directly attached.

All static routes that specify the same values for **vrf** *vrf-name*, *interface-type interface-number* , and *ipv6-address* will automatically use BFDv6 to determine gateway reachability and take advantage of fast failure detection.

Examples

The following example creates a neighbor on Ethernet interface 0/0 with an address of 2001::1:

```
Router(global config)# ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Router(global config)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

Related Commands

Command	Description
show ipv6 static	Displays the current contents of the IPv6 routing table.

ipv6 route static resolve default

To allow a recursive IPv6 static route to resolve using the default IPv6 static route, use the **ipv6 route static resolve default**command in global configuration mode. To remove this function, use the **no** form of this command.

ipv6 route static resolve default
no ipv6 route static resolve default

Syntax Description

This command has no arguments or keywords.

Command Default

Recursive IPv6 static routes do not resolve via the default route.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

By default, a recursive IPv6 static route will not resolve using the default route (::/0). The **ipv6 route static resolve default** command restores legacy behavior and allows resolution using the default route.

Examples

The following example enables an IPv6 recursive static route to be resolved using a IPv6 static default route:

```
Router(config)# ipv6 route static resolve default
```

ipv6 router eigrp

To place the router in router configuration mode, create an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process in IPv6, and configure this process, use the **ipv6**router **eigrp**command in global configurationmode. To shut down a routing process, use the **no** form of this command.

ipv6 router eigrp *as-number* [**eigrp event-log-size event-log-size**]
no ipv6 router eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
eigrp event-log-size *event-log-size*	(Optional) Memory allocation value of the EIGRP event. The *event-log-size* value is the memory allocation, in bytes, calculated dynamically based on available memory. The *event-log-size* value is between 0 and the dynamically calculated number.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	The **eigrp event-log-size** keyword and *event-log-size* argument were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **ipv6 router eigrp** command in global configuration mode to place the router in router configuration mode and create a routing process. Once in router configuration mode, you can configure the EIGRP for IPv6 routing process using the **ipv6 router eigrp** command.

Examples

The following example places the router in router configuration mode and allows you to configure an EIGRP for IPv6 routing process:

```
Router(config)# ipv6 router eigrp 400
 eigrp router-id 10.13.14.15
 eigrp stub connected summary
 eigrp event-log-size 1000
 no shutdown
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.
router eigrp	Configures the EIGRP process.

ipv6 router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IPv6 on an interface and to attach an area designator to the routing process, use the **ipv6 router isis**command in interface configuration mode. To disable IS-IS for IPv6, use the **no**form of the command.

ipv6 router isis *area-name*
no ipv6 router isis *area-name*

Syntax Description

area-name	Meaningful name for a routing process. If a name is not specified, a null name is assumed and the process is referenced with a null name. This name must be unique among all IP or Connectionless Network Service (CLNS) device processes for a given device. Required for multiarea IS-IS configuration. Each area in a multiarea configuration should have a nonnull area name to facilitate identification of the area. Optional for conventional IS-IS configuration.

Command Default

No routing processes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Before the IPv6 IS-IS routing process can be configured, IPv6 routing must be enabled using the **ipv6 unicast-routing** global configuration command, and an IPv6 address must be configured on an interface using either the **ipv6 enable** interface configuration command or the the **ipv6 address** interface configuration command. The **ipv6 enable**command will automatically configure an IPv6 link-local address on the interface.

Examples

The following example specifies IS-IS as an IPv6 routing protocol for a process named Finance. The Finance process will run over the Fast Ethernet interface 0/1.

```
Device(config)# router isis Finance
Device(config-router)# net 49.0001.aaaa.aaaa.aaaa.00
Device(config-router)# exit
Device(config)# interface FastEthernet 0/1
Device(config-if)# ipv6 router isis Finance
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 enable	Enables an interface for IPv6 processing and automatically assigns an IPv6 link-local address on the interface.
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
net	Configures an IS-IS NET for a CLNS routing process.
router isis	Enables the IPv4 IS-IS routing protocol.

ipv6 router nemo

To enable the network mobility (NEMO) routing process on the home agent and place the router in router configuration mode, use the **ipv6 router nemo**command in global configuration mode. To disable this function, use the **no** form of the command.

ipv6 router nemo
no ipv6 router nemo

Syntax Description

This command has no arguments or keywords.

Command Default

The NEMO routing process is not enabled on the home agent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command enables the NEMO routing process on the home agent.

Examples

In the following example, NEMO is enabled on the home agent:

```
Router(config)# ipv6 router nemo
```

ipv6 router ospf

To enable Open Shortest Path First (OSPF) for IPv6 router configuration mode, use the ipv6 **router ospf** command in global configuration mode.

ipv6 router ospf *process-id*

Syntax Description

process-id	Internal identification. It is locally assigned and can be a positive integer from 1 to 65535. The number used here is the number assigned administratively when enabling the OSPF for IPv6 routing process.

Command Default

No OSPF for IPv6 routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. It was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.
12.2(50)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 12.2(50)SY.
15.0(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.0(1)SY.
15.0(2)SE	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.0(2)SE.

Release	Modification
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Use this command to enter the OSPF for IPv6 router configuration mode. From this mode, you can enter several commands to customize OSPF for IPv6.

Examples

The following example enables the device with OSPF for IPv6 configuration mode and identifies the process with the number 1:

```
ipv6 router ospf 1
```

ipv6 router rip

To configure an IPv6 Routing Information Protocol (RIP) routing process, use the **ipv6 route r rip** command in global configuration mode. To remove a routing process, use the **no** form of this command.

ipv6 router rip *word*
no ipv6 router rip *word*

Syntax Description

word	A word that describes the routing process.

Command Default

No IPv6 RIP routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.6.0E	This command was integrated into Cisco IOS XE Release 3.6.0E. This command is modified. When this command is used in VRF-mode, only one process is created.

Usage Guidelines

The **ipv6 router rip**command is similar to the **router rip**command, except that it is IPv6-specific.

Use this command to enable an IPv6 RIP routing process. Configuring this command places the router in router configuration mode for the IPv6 RIP routing process. The router prompt changes to Router(config-rtr-rip)#.

When this command is used in VRF mode,

Examples

The following example configures the IPv6 RIP routing process named cisco and places the router in router configuration mode for the IPv6 RIP routing process:

```
Router(config)# ipv6 router rip cisco
```

Related Commands

Command	Description
ipv6 rip enable	Enables an IPv6 RIP routing process on an interface.

ipv6 routing-enforcement-header loose

To provide backward compatibility with legacy IPv6 inspection, use the ipv6 routing-enforcement-header loose command in parameter map type inspect configuration mode. To disable this feature, use the **no** form of this command.

ipv6 routing-enforcement-header loose
no ipv6 routing-enforcement-header loose

Syntax Description

This command has no arguments or keywords.

Command Default

Backward compatibility is not provided.

Command Modes

parameter map type inspect configuration mode (config-profile)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **ipv6 routing-enforcement-header loose** command provides backward compatibility with legacy IPv6 inspection. Enabling this command ensures that the firewall will not drop IPv6 traffic with routing headers. The default firewall behavior is to drop all IPv6 traffic without a routing header.

Examples

The following example enables backward compatibility with legacy IPv6 inspection on an inspect type parameter map named v6-param-map:

```
Router(config)# parameter-map type inspect v6-param-map
Router (config-profile)# ipv6 routing-header-enforcement loose
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

ipv6 snooping attach-policy

To apply an IPv6 snooping policy to a target, use the **ipv6 snooping attach-policy** command in IPv6 snooping configuration mode, or interface configuration mode. To remove a policy from a target, use the **no** form of this command.

ipv6 snooping policy attach-policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not attached to a target.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Once a policy has been identified or configured, it is applied on a target using the **ipv6 snooping attach-policy** command. This command is applied on any target, which varies depending on the platform. Examples of targets (depending on the platform used) include device ports, switchports, Layer 2 interfaces, Layer 3 interfaces, and VLANs.

Examples

The following examples shows how to apply an IPv6 snooping policy named policy1 to a target:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
```

Related Commands

Command	Description
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

ipv6 snooping logging

To configure IPv6 snooping security logging, use the **ipv6 snooping logging** command in global configuration mode. To disable IPv6 snooping security logging, use the **no** form of this command.

ipv6 snooping logging packet drop
no ipv6 snooping logging packet drop

Syntax Description

packet drop	Enables logging of router advertisements (RAs) dropped.

Command Default

Snooping security logging is not enabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping logging** command with the **packet** and **drop** keywords to log RAs that are dropped when they are received on an unauthorized port.

Examples

The following example enables the router to log RAs received on an unauthorized port:

```
Router (config)# ipv6 snooping logging packet drop
```

Related Commands

Command	Description
<<**command**>>	<<FID.>>

ipv6 snooping logging packet drop

To enable the logging of dropped packets by the IPv6 first-hop security feature, use the **ipv6 snooping logging packet drop**command in global configuration mode. To disable the logging of dropped packets by the IPv6 first-hop security feature, use the **no** form of this command.

ipv6 snooping logging packet drop
no ipv6 snooping logging packet drop

Syntax Description

This command has no arguments or keywords.

Command Default

Snooping security logging is not enabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping logging packet drop**command to log packets that are dropped when they are received on an unauthorized port. For example, this command will log RA packets that are dropped because of the RA guard feature.

Related Commands

Command	Description
ipv6 neighbor binding logging	Enables the logging of binding table main events.

ipv6 snooping policy

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **data-glean**/**destination-glean** command enables IPv6 first-hop security binding table recovery using data or destination address gleaning.
- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- **security-level** specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

Once a policy has been identified or configured, it is applied on a device using the **ipv6 snooping attach-policy** command.

Examples

The following examples show how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
```

Related Commands

Command	Description
ipv6 snooping attach-policy	Applies an IPv6 snooping policy to a target.

ipv6 source-guard attach-policy

To apply IPv6 source guard policy on an interface, use the **ipv6 source-guard attach-policy** in interface configuration mode. To remove this source guard from the interface, use the **no** form of this command.

ipv6 source-guard attach-policy [*source-guard-policy*]

Syntax Description

source-guard-policy	(Optional) User-defined name of the source guard policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 source-guard policy is not applied on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

If no policy is specified using the *source-guard-policy* argument, then the default source-guard policy is applied.

A dependency exists between IPv6 source guard and IPv6 snooping. Whenever IPv6 source guard is configured, when the **ipv6 source-guard attach-policy** command is entered, it verifies that snooping is enabled and issues a warning if it is not. If IPv6 snooping is disabled, the software checks if IPv6 source guard is enabled and sends a warning if it is.

Examples

The following example shows how to apply IPv6 source guard on an interface:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

Related Commands

Command	Description
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

ipv6 source-guard policy

To configure an IPv6 source-guard policy and enter source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode, use the **ipv6 source-guard policy** command in global configuration mode. To remove an IPv6 source-guard policy, use the **no** form of this command.

ipv6 source-guard policy *source-guard-policy*
no ipv6 source-guard policy *source-guard-policy*

Syntax Description

source-guard-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 source-guard policy is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **ipv6 source-guard policy** command to define a source-guard policy name and enter source-guard policy configuration mode.

The administrator can use the following commands to configure the policy:

- The **permit link-local** command allows hardware bridging for all data traffic sourced by a link-local address.
- The **deny global-autoconf** command denies data traffic from auto-configured global addresses.

Examples

```
Device(config)# ipv6 source-guard policy policy1
Device(config-source-guard)#
```

Related Commands

Command	Description
deny global-autoconfig	Denies data traffic from autoconfigured global addresses.
permit link-local	Allows hardware bridging for all data traffic sourced by a link-local address.

ipv6 source-route

To enable processing of the IPv6 type 0 routing header (the IPv6 source 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 arguments or keywords.

Command Default

The **no** version of the **ipv6 source-route** command is the default. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 Internet Control Message Protocol (ICMP) error message back to the source and logs an appropriate debug message.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.4(15)T	The default was changed to be the **no** version of the **ipv6 source-route** command. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.
12.2(33)SRC	Changes made to this command were integrated into Cisco IOS 12.2(33)SRC.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The default was changed to be the **no** version of the **ipv6 source-route** command, which means this functionality is not enabled. Before this change, this functionality was enabled automatically. User who had configured the **no ipv6 source-route** command before the default was changed will continue to see this configuration in their **show config** command output, even though the **no** version of the command is the default.

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 type0 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.

In IPv6, source routing is performed only by the destination of the packet. Therefore, in order to stop source routing from occurring inside your network, you need to configure an IPv6 access control list (ACL) that includes the following rule:

```
deny ipv6 any any routing
```

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval**command.

Examples

The following example disables the processing of IPv6 type 0 routing headers:

```
no ipv6 source-route
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 spd mode

To configure an IPv6 Selective Packet Discard (SPD) mode, use the **ipv6 spd mode**command in global configuration mode. To remove the IPv6 SPD mode, use the **no** form of this command.

ipv6 spd mode {**aggressive** | **tos protocol ospf**}
no ipv6 spd mode {**aggressive** | **tos protocol ospf**}

Syntax Description

aggressive	Aggressive drop mode discards incorrectly formatted packets when the IPv6 SPD is in random drop state.
tos protocol o spf	OSPF mode allows OSPF packets to be handled with SPD priority.

Command Default

No IPv6 SPD mode is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The default setting for the IPv6 SPD mode is none, but you may want to use the **ipv6 spd mode** command to configure a mode to be used when a certain SPD state is reached.

The **aggressive** keyword enables aggressive drop mode, which drops deformed packets when IPv6 SPD is in random drop state. The **ospf** keyword enables OSPF mode, in which OSPF packets are handled with SPD priority.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to enable the router to drop deformed packets when the router is in the random drop state:

```
Router(config)# ipv6 spf mode aggressive
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.

Command	Description
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 spd queue max-threshold

To configure the maximum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the **ipv6 spd queue max-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 spd queue max-threshold *value*
no ipv6 spd queue max-threshold

Syntax Description

value	Number of packets. The range is from 0 through 65535.

Command Default

No SPD queue maximum threshold value is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was modified. The *value* argument range was changed from 4096 through 65535 to 0 through 65535.

Usage Guidelines

Use the **ipv6 spd queue max-threshold** command to configure the SPD queue maximum threshold value.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to set the maximum threshold value of the queue to 60,000:

```
Router(config)# ipv6 spd queue max-threshold 60000
```

Related Commands

Command	Description
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 spd queue min-threshold

To configure the minimum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the **ipv6 spd queue min-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 spd queue min-threshold *value*
no ipv6 spd queue min-threshold

Syntax Description

value	Number of packets. The range is from 0 through 65535.

Command Default

No SPD queue minimum threshold is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **ipv6 spd queue min-threshold** command to configure the SPD queue minimum threshold, which determines IPv6 state transition from normal to random drop state. The minimum threshold value must be lower than the maximum threshold setting.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to set the IPv6 SPD minimum threshold to 4094 packets:

```
Router(config)# ipv6 spd queue min-threshold 4094
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 split horizon, use the **ipv6**split-horizon **eigrp**command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *as-number*
no ipv6 split-horizon eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP for IPv6 split horizon is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

For networks that include links over X.25 packet-switched networks (PSNs), you can use the **neighbor** command in router configuration mode to disable the split horizon feature. Or, you can specify the **no ipv6 split-horizon eigrp** command in your configuration. However, if you do disable the split horizon feature, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Note In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change in order to advertise routes properly. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0
 encapsulation x25
 no ipv6 split-horizon eigrp 101
```

Related Commands

Command	Description
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information on a router that is running EIGRP.

IPv6 Commands: ipv6 su to m

ipv6 summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ipv6**summary-address **eigrp**command in interface configuration mode. To disable a configuration, use the **no** form of this command.

ipv6 summary-address eigrp *as-number* *ipv6-address* [*admin-distance*]
no ipv6 summary-address eigrp *as-number* *ipv6-address* [*admin-distance*]

Syntax Description

as-number	Autonomous system number.
ipv6-address	Summary IPv6 address to apply to an interface.
admin-distance	(Optional) Administrative distance. A value from 0 through 255. The default value is 90.

Command Default

An administrative distance of 5 is applied to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 summary routes. EIGRP for IPv6 automatically summarizes to the network level, even for a single host route. No summary addresses are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **ipv6 summary-address eigrp** command is used to configure interface-level address summarization. EIGRP for IPv6 summary routes are given an administrative distance value of 5. The administrative distance metric is used to advertise a summary address without installing it in the routing table.

Examples

The following example provides a summary aggregate address for EIGRP for IPv6 for AS 1:

```
ipv6 summary-address eigrp 1 2001:0DB8:0:1::/64
```

ipv6 tacacs source-interface

To specify an interface to use for the source address in TACACS packets, use the **ipv6 tacacs source-interface**command in global configuration mode. To remove the specified interface from the configuration, use the **no** form of this command.

ipv6 tacacs source-interface *interface* **vrf** *vrf-name*
no ipv6 tacacs source-interface *interface*

Syntax Description

interface	Interface to be used for the source address in TACACS packets.
vrf *vrf-name*	VPN routing/forwarding parameter name.

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
Cisco IOS XE Fuji 16.9.1	The **vrf** *vrf-name* keyword-argument pair was added.

Usage Guidelines

The **ipv6 tacacs source-interface**command specifies an interface to use for the source address in TACACS packets.

Examples

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in TACACS packets:

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

ipv6 traffic interface-statistics

To collect IPv6 forwarding statistics for all interfaces, use the **ipv6 traffic interface-statistics**command in global configuration mode. To ensure that IPv6 forwarding statistics are not collected for any interface, use the **no** form of this command.

ipv6 traffic interface-statistics [**unclearable**]
no ipv6 traffic interface-statistics [**unclearable**]

Syntax Description

unclearable	(Optional) IPv6 forwarding statistics are kept for all interfaces, but it is not possible to clear the statistics on any interface.

Command Default

IPv6 forwarding statistics are collected for all interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Using the optional unclearable keyword halves the per-interface statistics storage requirements.

Examples

The following example does not allow statistics to be cleared on any interface:

```
ipv6 traffic interface-statistics unclearable
```

ipv6 traffic-filter

To filter incoming or outgoing IPv6 traffic on an interface, use the **ipv6 traffic-filter**command in interface configuration mode. To disable the filtering of IPv6 traffic on an interface, use the **no** form of this command.

ipv6 traffic-filter *access-list-name* {**in** | **out**}
no ipv6 traffic-filter *access-list-name*

Syntax Description

access-list-name	Specifies an IPv6 access name.
in	Specifies incoming IPv6 traffic.
out	Specifies outgoing IPv6 traffic.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.2(33)SXI4	The **out** keyword and therefore filtering of outgoing traffic is not supported in IPv6 port-based access list (PACL) configuration.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.
12.2(50)SY	This command was modified. The **out** keyword is not supported.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Examples

The following example filters inbound IPv6 traffic on Ethernet interface 0/0 as defined by the access list named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 traffic-filter cisco in
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing**command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

ipv6 unicast-routing
no ipv6 unicast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 unicast routing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Configuring the **no ipv6 unicast-routing** command removes all IPv6 routing protocol entries from the IPv6 routing table.

Examples

The following example enables the forwarding of IPv6 unicast datagrams:

```
Device(config)# ipv6 unicast-routing
```

Related Commands

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

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 unnumbered

To enable IPv6 processing on an interface without assigning an explicit IPv6 address to the interface, use the **ipv6 unnumbered**command in interface configuration mode. To disable IPv6 on an unnumbered interface, use the **no** form of this command.

ipv6 unnumbered *interface-type* **interface-number**
no ipv6 unnumbered

Syntax Description

interface-type	The interface type of the source address that the unnumbered interface uses in the IPv6 packets that it originates. The source address cannot be another unnumbered interface.
interface-number	The interface number of the source address that the unnumbered interface uses in the IPv6 packets that it originates.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

IPv6 packets that are originated from an unnumbered interface use the global IPv6 address of the interface specified in the **ipv6 unnumbered** command as the source address for the packets. The **ipv6 unnumbered** *interface* command is used as a hint when doing source address selection; that is, when trying to determine the source address of an outgoing packet.

Note Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and tunnel interfaces can be unnumbered. You cannot use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.

Examples

The following example configures serial interface 0/1as unnumbered. IPv6 packets that are sent on serial interface 0/1 use the IPv6 address of Ethernet 0/0 as their source address:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 3FFE:C00:0:1:260:3EFF:FE11:6770
Router(config)# interface serial 0/1
Router(config-if)# ipv6 unnumbered ethernet 0/0
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 unreachables

To enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface, use the **ipv6 unreachables** command in interface configuration mode. To prevent the generation of unreachable messages, use the **no** form of this command.

ipv6 unreachables
no ipv6 unreachables

Syntax Description

This command has no arguments or keywords.

Command Default

ICMPv6 unreachable messages can be generated for any packets arriving on that interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 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.

Examples

The following example enables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ipv6 unreachables
```

ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ipv6 verify unicast reverse-path [**access-list** *name*]
no ipv6 verify unicast reverse-path [**access-list** *name*]

Syntax Description

access-list *name*	(Optional) Specifies the name of the access list. **Note** This keyword and argument are not supported on the Cisco 12000 series Internet router.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and introduced on the 10G Engine 5 SPA Interface Processor in the Cisco 12000 series Internet router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in strict checking mode. The Unicast RPF for IPv6 feature requires that Cisco Express Forwarding for IPv6 is enabled on the router.

Note Beginning in Cisco IOS Release 12.0(31)S, the Cisco 12000 series Internet router supports both the **ipv6 verify unicast reverse-path** and **ipv6 verify unicast source reachable-via rx** commands to enable Unicast RPF to be compatible with the Cisco IOS Release 12.3T and 12.2S software trains.

Use the **ipv6 verify unicast reverse-path** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source IPv6 address appears in the routing table and that it is reachable by a path through the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.

The Unicast RPF feature performs a reverse lookup in the CEF table to check if any packet received at a router interface has arrived on a path identified as a best return path to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast RPF command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Note When you configure Unicast RPF for IPv6 on the Cisco 12000 series Internet router, the most recently configured checking mode is not automatically applied to all interfaces as on other platforms. You must enable Unicast RPF for IPv6 separately on each interface. When you configure a SPA on the Cisco 12000 series Internet router, the interface address is in the format *slot/subslot/port*. The optional **access-list** keyword for the **ipv6 verify unicast reverse-path** command is not supported on the Cisco 12000 series Internet router. For information about how Unicast RPF can be used with ACLs on other platforms to mitigate the transmission of invalid IPv4 addresses (perform egress filtering) and to prevent (deny) the reception of invalid IPv4 addresses (perform ingress filtering), refer to the "Configuring Unicast Reverse Path Forwarding" chapter in the "Other Security Features" section of the *Cisco IOS Security Configuration Guide*.

Note When using Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on).

Do not use Unicast RPF on core-facing interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Apply Unicast RPF only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples

Unicast Reverse Path Forwarding on a Serial Interface

The following example shows how to enable the Unicast RPF feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

Unicast Reverse Path Forwarding on a Cisco 12000 Series Internet Router

The following example shows how to enable Unicast RPF for IPv6 with strict checking on a 10G SIP Gigabit Ethernet interface 2/1/2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitEthernet 2/1/2
Router(config-if)# ipv6 verify unicast reverse-path
Router(config-if)# exit
```

Unicast Reverse Path Forwarding on a Single-Homed ISP

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
interface Serial 5/0/0
description Connection to Upstream ISP
ipv6 address FE80::260:3EFF:FE11:6770/64
no ipv6 redirects
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 host 2::1 any
deny ipv6 FEC0::/10 any
  ipv6 access-group abc in
  ipv6 access-group jkl out
!
access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001any
access-list abc deny ipv6 any any log
access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5.255.255.255 any log
access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5172.16.0.0
0.15.255.255 any log
access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
access-list jkl permit ipv6
```

ACL Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL "abc." In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 1234:5678::1 arriving at Ethernet interface 0/0 are forwarded because of the permit statement in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
interface ethernet 0/0
ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
permit ipv6 1234:5678::/64 any log-input
deny ipv6 8765:4321::/64 any log-input
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip verify unicast reverse-path	Enables Unicast RPF for IPv4 traffic.
ipv6 cef	Enables Cisco Express Forwarding for IPv6 interfaces.

ipv6 verify unicast source reachable-via

To verify that a source address exists in the FIB table and enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ipv6 verify unicast source reachable-via** command in interface configuration mode. To disable URPF, use the **no** form of this command.

ipv6 verify unicast source reachable-via {**rx** | **any**} [**allow-default**] [*access-list-name*]
no ipv6 verify unicast

Syntax Description

rx	Source is reachable through the interface on which the packet was received.
any	Source is reachable through any interface.
allow-default	(Optional) Allows the lookup table to match the default route and use the route for verification.
access-list-name	(Optional) Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeral.

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **ipv6 verify unicast reverse-path** command is used to enable Unicast RPF for IPv6 in loose checking mode.

Use the **ipv6 verify unicast source reachable-via**command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

The URPF feature checks to see if any packet received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the CEF table. If URPF does not find a reverse path for the packet, U RPF can drop or forward the packet, depending on whether an access control list (ACL) is specified in the **ipv6 verify unicast source reachable-via** command. If an ACL is specified in the command, then when (and only when) a packet fails the URPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for U RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ipv6 verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

U RPF events can be logged by specifying the logging option for the ACL entries used by the **ipv6 verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Examples

The following example enables Unicast RPF on any interface:

```
ipv6 verify unicast source reachable-via any
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 virtual-reassembly

To enable Virtual Fragment Reassembly (VFR) on an interface, use the **ipv6 virtual-reassembly** command in global configuration mode. To remove VFR configuration, use the **no** form of this command.

ipv6 virtual-reassembly [{**in** | **out**}] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**]
no ipv6 virtual-reassembly [{**in** | **out**}] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**]

Syntax Description

in	(Optional) Enables VFR on the ingress direction of the interface.
out	(Optional) Enables VFR on the egress direction of the interface.
max-reassemblies *maxreassemblies*	(Optional) Sets the maximum number of concurrent reassemblies (fragment sets) that the Cisco IOS software can handle at a time. The default value is 64.
max-fragments *max-fragments*	(Optional) Sets the maximum number of fragments allowed per datagram (fragment set). The default is 16.
timeout *seconds*	(Optional) Sets the timeout value of the fragment state. The default timeout value is 2 seconds. If a datagram does not receive all its fragments within 2 seconds, all of the fragments received previously will be dropped and the fragment state will be deleted.
drop-fragments	(Optional) Turns the drop fragments feature on or off.

Command Default

Max-reassemblies = 64 Fragments = 16 If neither the **in** or **out** keyword is specified, VFR is enabled on the ingress direction of the interface only.**drop-fragments** keyword is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
15.1(1)T	The **in** and **out** keywords were added. • The **out** keyword must be used to configure or disable the egress direction of the interface.
Cisco IOS XE Release 3.4S	The **drop-fragments** keyword was added.

Usage Guidelines

When the **ipv6 virtual-reassembly** command is configured on an interface without using one of the command keywords, VFR is enabled on the ingress direction of the interface only. In Cisco IOS XE Release 3.4S, all VFR-related alert messages are suppressed by default.

Maximum Number of Reassemblies

Whenever the maximum number of 256 reassemblies (fragment sets) is crossed, all the fragments in the forthcoming fragment set will be dropped and an alert message VFR-4-FRAG_TABLE_OVERFLOW will be logged to the syslog server.

Maximum Number of Fragments per Fragment Set

If a datagram being reassembled receives more than eight fragments then, tall fragments will be dropped and an alert message VFR-4-TOO_MANY_FRAGMENTS will be logged to the syslog server.

Explicit Removal of Egress Configuration

As of the Cisco IOS 15.1(1)T release, the **no ipv6 virtual-reassembly** command, when used without keywords, removes ingress configuration only. To remove egress interface configuration, you must enter the **out** keyword.

Examples

The following example configures the ingress direction on the interface. It sets the maximum number of reassemblies to 32, maximum fragments to 4, and the timeout to 7 seconds:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7
```

The following example enables the VFR on the ingress direction of the interface. Note that even if the **in** keyword is not used, the configuration default is to configure the ingress direction on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly in
```

The following example enables egress configuration on the interface. Note that the **out** keyword must be used to enable and disable egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly out
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly out
end
```

The following example disables egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# no
 ipv6 virtual-reassembly out
Router(config-if)# end
```

ipv6 virtual-reassembly drop-fragments

To drop all fragments on an interface, use the **ipv6 virtual-reassembly drop-fragments** command in global configuration mode. Use the **no** form of this command to remove the packet-dropping behavior.

ipv6 virtual-reassembly drop-fragments
no ipv6 virtual-reassembly drop-fragments

Syntax Description

This command has no arguments or keywords.

Command Default

Fragments on an interface are not dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example causes all fragments on an interface to be dropped:

```
ipv6 virtual-reassembly drop-fragments
```

ipv6 wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ipv6 wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

ipv6 wccp vrf *vrf-name* {**web-cache***service-number*} [**service-list** *service-access-list*] [**mode** {**open** | **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [{**0** | **7**}] *password*]
no ipv6 wccp vrf *vrf-name* {**web-cache***service-number*} [**service-list** *service-access-list*] [**mode** {**open** | **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [{**0** | **7**}] *password*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
web-cache	Specifies the web-cache service. **Note** Web cache is one of the services. The maximum number of services, including those assigned with the *service-number* argument, is 256.
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword. **Note** If Cisco cache engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
service-list *service-access-list*	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
mode open	(Optional) Identifies the service as open. This is the default service mode.
mode closed	(Optional) Identifies the service as closed.
group-address *multicast-address*	(Optional) Specifies the multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which web cache should receive redirected messages.
redirect-list *access-list*	(Optional) Specifies the access list that controls traffic redirected to this service group. The *access-list* argument should consist of a string of no more than 64 characters (name or number) in length that specifies the access list.
group-list *access-list*	(Optional) Specifies the access list that determines which web caches are allowed to participate in the service group. The *access-list* argument specifies either the number or the name of a standard or extended access list.

password [**0** | **7**] *password*	(Optional) Specifies the message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The *password* argument can be up to eight characters in length.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwardin) switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ipv6 wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by specifying the **ipv6 wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a router to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

The **vrf** *vrf-name* keyword and argument pair is optional. It allows you to specify a VRF to associate with a service group. You can then specify a web-cache service name or service number.

The same service (web-cache or service number) can be configured in different VRF tables. Each service will operate independently.

When the **no ipv6 wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still has the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command.

ipv6 wccp [vrf *vrf-name*] {web-cache | *service-number*} group-address *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received on this group address. The response also is sent to the group address. The default is for no group address to be configured, in which case all "Here I Am" messages are responded to with a unicast reply.

ipv6 wccp [vrf *vrf-name*] {web-cache | *service-number*} redirect-list *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either the number or the name of a standard or extended access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- UDP (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and web caches.
- Generic routing encapsulation (GRE) (protocol type 47 encapsulated frames). Blocking this type of traffic will prevent the web caches from ever seeing the packets that are intercepted.

ipv6 wccp [vrf *vrf-name*] {web-cache | *service-number*} group-list *access-list*

This option instructs the router to use an access list to control the web caches that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named access list. The access list itself specifies which web caches are permitted to participate in the service group. The default is for no group list to be configured, in which case all web caches may participate in the service group.

Note The **ipv6 wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ipv6 wccp** {**web-cache** | *service-number*} **group-listen** command, but these are entirely different commands. The **ipv6 wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **ipv6 wccp group-listen** command in the *Cisco IOS IP Application Services Command Reference*.

ipv6 wccp [vrf *vrf-name*] web-cache | *service-number*} password *password*

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the router. You must also configure the same password separately on each web cache. The password can be up to a maximum of eight characters in length. Messages that do not authenticate when authentication is enabled on the router are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

ipv6 wccp *service-number* service-list*service-access-list* mode closed

In applications where the interception and redirection of WCCP packets to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, it is necessary to block packets for the application when the intermediary device is not available. This blocking is called a closed service. By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device. The **service-list** keyword can only be used for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When the definition of a service in a service list conflicts with the definition received via the WCCP protocol, a warning message similar to the following is displayed:

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client 10.1.1.13
```

When there is a conflict in service list definitions, the configured definition takes precedence over the external definition received via WCCP protocol messages.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 wccp 99 group-address 239.0.0.0
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp 99 group-listen
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
Router(config)# access-list 100 deny ip any host 10.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ipv6 wccp web-cache redirect-list 100
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp web-cache redirect out
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving Fast Ethernet interface 0/0. Because the outbound access control list (ACL) check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Router(config)# ipv6 wccp web-cache
Router(config)# ipv6 wccp check acl outbound
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 10 out
Router(config-if)# ipv6 wccp web-cache redirect out
Router(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config-if)# access-list 10 permit any
```

If the outbound ACL check is disabled, HTTP packets from network 10.0.0.0 would be redirected to a cache, and users with that network address could retrieve web pages when the network administrator wanted to prevent this from happening.

The following example shows how to configure a closed WCCP service:

```
Router(config)# ipv6 wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
ipv6 wccp check services all	Enables all WCCP services.
ipv6 wccp redirect excludein	Configures an interface to exclude packets received on an interface from being checked for redirection.
show ipv6 wccp	Displays global statistics related to WCCP.

ipv6 wccp check acl outbound

To check the access control list (ACL) for egress interfaces for packets redirected by the Web Cache Communication Protocol (WCCP), use the **ipv6 wccp check acl outbound** command in global configuration mode. To disable the outbound check for redirected packets, use the **no** form of this command.

ipv6 wccp check acl outbound
no ipv6 wccp check acl outbound

Syntax Description

This command has no arguments or keywords.

Command Default

Check of the outbound ACL services is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

This command enables the outbound check for redirected packets.

Examples

The following example shows how to configure a router to check the ACL for the egress interfaces for inbound packets that are redirected by WCCP:

```
Router(config)# ipv6 wccp check acl outbound
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.
ipv6 wccp check services all	Enables all WCCP services.

ipv6 wccpcheck services all

To enable all Web Cache Communication Protocol (WCCP) services, use the **ipv6 wccp check services all** command in global configuration mode. To disable all services, use the **no** form of this command.

ipv6 wccp check services all
no ipv6 wccp check services all

Syntax Description

This command has no arguments or keywords.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

With the **ipv6 wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect access control list (ACL) and by the priority value of the service.

An interface can be configured with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found that matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ipv6 wccp check services all** command is configured. When the **ipv6 wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

Note The priority of a WCCP service group is determined by the web cache appliance. The priority of a WCCP service group cannot be configured via Cisco IOS software.

Note The **ipv6 wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Examples

The following example shows how to configure all WCCP services:

```
Router(config)# ipv6 wccp check services all
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.

ipv6 wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP), use the **ipv6 wccp group-listen** command in interface configuration mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

ipv6 wccp [**vrf** *vrf-name*] {**web-cache***service-number*} **group-listen**
no ipv6 wccp [**vrf** *vrf-name*] {**web-cache***service-number*} **group-listen**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
web-cache	Directs the router to send packets to the web cache service.
service-number	WCCP service number; valid values are from 0 to 254.

Command Default

No interface is configured to enable the reception of IP multicast packets for WCCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Note the following requirements on routers that are to be members of a service group when IP multicast is used:

- Configure the IP multicast address for use by the WCCP service group.
- Enable IP multicast routing using the **ipv6 multicast-routing** command in global configuration mode.
- Configure the interfaces on which the router wants to receive the IP multicast address with the **ipv6 wccp** {**web-cache** | *service-number*} **group-listen** interface configuration command.

Examples

The following example shows how to enable the multicast packets for a web cache with a multicast address of 2001:DB8:100::1:

```
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 wccp web-cache group-address 2001:DB8:100::1
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp web-cache group-listen
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing.

Command	Description
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables WCCP redirection on an interface.

ipv6 wccp redirect

To enable packet redirection on an outbound or inbound interface using the Web Cache Communication Protocol (WCCP), use the **ipv6 wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

ipv6 wccp [**vrf** *vrf-name*] {**web-cache***service-number*} **redirect** {**in** | **out**}
no ipv6 wccp [**vrf** *vrf-name*] {**web-cache***service-number*} **redirect** {**in** | **out**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
web-cache	Enables the web cache service.
service-number	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Command Default

Redirection checking on the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the Content Engine interface, and specify the **ipv6 wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by specifying the **ipv6 wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ipv6 wccp** command for configuration of the redirect list and service group.

The **ipv6 wccp redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ipv6 wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Tip Be careful not to confuse the **ipv6 wccp redirect** {**out** | **in** } interface configuration command with the **ipv6 wccp redirect exclude in** interface configuration command.

Note This command has the potential to affect the **ipv6 wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ipv6 wccp redirect exclude in** set on an interface and you subsequently configure the **ipv6 wccp redirect in** command, the **exclude in** command will be overridden. The opposite is also true: Configuring the **exclude in** command will override the **redirect in** command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when Cisco Express Forwarding switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ipv6 address 2001:DB8:100::1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ipv6 wccp web-cache redirect out
Router(config-if)# ipv6 nat outside
Router(config-if)# ipv6 inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 2
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ipv6 wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
Router(config)# ipv6 wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ipv6 wccp web-cache redirect in
```

Related Commands

Command	Description
ipv6 wccp redirect exclude in	Enables redirection exclusion on an interface.
show ipv6 interface	Displays the usability status of interfaces that are configured for IP.

Command	Description
show ipv6 wccp	Displays the WCCP global configuration and statistics.

ipv6 wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ipv6 wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ipv6 wccp redirect exclude in
no ipv6 wccp redirect exclude in

Syntax Description

This command has no arguments or keywords.

Command Default

Redirection exclusion is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

This configuration command instructs the interface to exclude inbound packets from any redirection check. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the Internet and to allow for the use of the WCCPv2 packet return feature.

Examples

In the following example, packets arriving on Ethernet interface 0 are excluded from all WCCP redirection checks:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 wccp redirect exclude in
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect out	Configures redirection on an interface in the outgoing direction.

ipv6 wccp source-interface

To specify the interface that Web Cache Communication Protocol (WCCP) uses as the preferred router ID and generic routing encapsulation (GRE) source address, use the **ipv6 wccp source-interface** command in global configuration mode. To enable the WCCP default behavior for router ID selection, use the **no** form of this command.

ipv6 wccp [**vrf** *vrf-name*] **source-interface** *source-interface*
no ipv6 wccp [**vrf** *vrf-name*] **source-interface**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
source-interface	The type and number of the source interface.

Command Default

If this command is not configured, WCCP selects a loopback interface with the highest IP address as the router ID. If a loopback interface does not exist, then the interface that WCCP uses as the preferred router ID and GRE source address cannot be specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Use this command to set the interface from which WCCP may derive the router ID and GRE source address. The router ID must be a reachable IPv6 address.

The interface identified by the *source-interface* argument must be assigned an IPv6 address and be operational before WCCP uses the address as the router ID. If the configured source interface cannot be used to derive the WCCP router ID, the configuration is ignored and a Cisco IOS error message similar to the following is displayed:

```
%WCCP-3-SIFIGNORED: source-interface interface
 ignored (reason)
```

The *reason* field in the error output indicates why the interface has been ignored and can include the following:

- **VRF mismatch**--The VRF domain associated with the interface does not match the VRF domain associated with the WCCP command.
- **interface does not exist**--The interface has been deleted.
- **no address**--The interface does not have a valid IPv6 address.
- **line protocol down**--The interface is not fully operational.

In the error case above, the source interface for the router ID will be selected automatically.

This command provides control only of the router ID and GRE source address. This command does not influence the source address used by WCCP control protocol ("Here I Am" and Removal Query messages). The WCCP control protocol is not bound to a specific interface and the source address is always selected based on the destination address of an individual packet.

Examples

The following example shows how to select Gigabit Ethernet interface 0/0/0 as the WCCP source interface:

```
Router(config)# ipv6 wccp source-interface gigabitethernet0/0/0
```

Related Commands

Command	Description
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.
show ipv6 wccp	Displays the WCCP global configuration and statistics.

isis ipv6 bfd

To enable or disable IPv6 Bidirectional Forwarding Detection (BFD) on a specific interface configured for Intermediate System-to-Intermediate System (IS-IS), use the **isis ipv6 bfd** command in interface configuration mode. To remove the IPv6 BFD configuration from the interface, use the **no** form of this command.

isis ipv6 bfd
[**disable**]
noisis ipv6 bfd
[**disable**]

Syntax Description

disable	(Optional) Disables IPv6 BFD for IS-IS on a specified interface.

Command Default

IPv6 BFD support for IS-IS is enabled on the interface.

Command Modes

Interface configuration (config-if)#

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Enter the **isis ipv6 bfd** command in interface configuration mode to configure an IS-IS interface to use IPv6 BFD for failure detection. If you have used the **bfd all-interfaces** command in router configuration mode to globally configure all IS-IS interfaces for an IS-IS process to use BFD, you can enter the **isis ipv6 bfd** command with the **disable** keyword in interface configuration mode to disable BFD for a specific IS-IS interface.

Entering the **no isis ipv6 bfd** command will remove the configuration from this IS-IS interface. In this case, whether or not an IS-IS interface for a particular IS-IS process is registered with the BFD protocol will depend on whether or not you have entered the **bfd all-interfaces** command in router configuration mode for the specific IS-IS process.

Examples

The following example enables IPv6 BFD on an IS-IS interface:

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# isis ipv6 bfd
```

Related Commands

Command	Description
ipv6 route priority high	Assigns a high priority to an IS-IS IPv6 prefix.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays additional information about the IS-IS database.

Command	Description
summary-prefix (IPv6 IS-IS)	Configures aggregate IPv6 prefixes for IS-IS.

isis ipv6 metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) IPv6 metric, use the **is is ipv6 metric** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

isis ipv6 metric {*metric-value* | **maximum**} [{**level-1** | **level-2**}]
no isis ipv6 metric {*metric-value* | **maximum**} [{**level-1** | **level-2**}]

Syntax Description

metric-value	Value added to the metric of an IPv6 IS-IS route received in a report message. The default metric value is 10. The range is from 1 to 16777214.
maximum	Excludes a link or adjacency from the Shortest Path Tree (SPF) calculation.
level-1	(Optional) Enables this command on routing Level 1. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.
level-2	(Optional) Enables this command on routing Level 2. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.

Command Default

The default metric value is set to 10.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.1	The **maximum** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **isis ipv6 metric** command is used only in multitopology IS-IS.

Changing the metric allows differentiation between IPv4 and IPv6 traffic, forcing traffic onto different interfaces. This function allows you to use the lower-cost rather than the high-cost interface.

For using extended metrics, such as with the IS-IS multitopology for IPv6 feature, Cisco IOS software provides support of a 24-bit metric field, the so-called "wide metric." Using the new metric style, link metrics now have a maximum value of 16777214 with a total path metric of 4261412864.

Cisco IOS Release 12.4(13) and 12.4(13)T

Entering the **maximum** keyword will exclude the link from the SPF calculation. If a link is advertised with the maximum link metric, the link will not be considered during the normal SPF computation. When the link excluded from the SPF, it will not be advertised for calculating the normal SPF. An example would be a link that is available for traffic engineering, but not for hop-by-hop routing. If a link, such as one that is used for traffic engineering, should not be included in the SPF calculation, enter the **isis ipv6 metric** command with the **maximum** keyword.

Note The **isis ipv6 metric maximum** command applies only when the **metric-style wide** command has been entered. The **metric-style wide**command is used to configure IS-IS to use the new-style type, length, value (TLV) because TLVs that are used to advertise IPv6 information in link-state packets (LSPs) are defined to use only extended metrics.

Examples

The following example sets the value of an IS-IS IPv6 metric to 20:

```
Router(config)# interface Ethernet 0/0/1
Router(config-if)# isis ipv6 metric 20
```

The following example sets the IS-IS IPv6 metric for the link to maximum. SPF will ignore the link for both Level 1 and Level 2 routing because neither the **level-1** keyword nor the **level-2** keyword was entered.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# isis ipv6 metric maximum
```

Related Commands

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style TLVs.

isis ipv6 tag

To configure an administrative tag value that will be associated with an IPv6 address prefix and applied to an Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP), use the **isis ipv6 tag** command in interface configuration mode. To remove a tag from the address prefix, use the **no** form of this command.

isis ipv6 tag *tag-value*
no isis ipv6 tag

Syntax Description

tag-value	The tag value. The range is from 1 to 4294967295.

Command Default

An administrative IPv6 IS-IS tag is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

No action occurs on a tagged route until the tag is used, for example, to redistribute routes or summarize routes.

Configuring the **isis ipv6 tag** command triggers the router to generate new LSPs because the tag is a new piece of information in the packet.

Examples

In the following example, the value of an IS-IS IPv6 administrative tag is set to 220:

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# isis ipv6 tag 220
```

Related Commands

Command	Description
ipv6 route priority high	Assigns a high priority to an IS-IS IPv6 prefix.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays additional information about the IS-IS database.
summary-prefix (IPv6 IS-IS)	Configures aggregate IPv6 prefixes for IS-IS.

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count**command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode .

limit address-count *maximum*

Syntax Description

maximum	Sets the role of the device to host.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size.

Use the **limit address-count**command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# limit address-count 25
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

log-adjacency-changes (OSPFv3)

To configure the router to send a syslog message when an Open Shortest Path First version 3 (OSPFv3) neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [**detail**]
no log-adjacency-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Command Default

This feature is enabled

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **log-adjacency changes** command to notify you when OSPFv3 neighbors go up or down. The **log-adjacency-changes** command provides a higher level view of those changes of the peer relationship with less output than **debug** commands provide. The **log-adjacency-changes** command is on by default, but only up/down (full/down) events are reported unless the **detail** keyword is also used.

Examples

The following example configures the router to send a syslog message when an OSPFv3 neighbor state changes:

```
Router(config-router)# log-adjacency-changes
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

log-neighbor-changes (IPv6 EIGRP)

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 neighbor adjacencies, use the **log-neighbor-changes** command in router configuration mode. To disable the logging of changes in EIGRP IPv6 neighbor adjacencies, use the **no** form of this command.

log-neighbor-changes
no log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The log-neighbor-changes command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.

Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the no form of this command.

Examples

The following example disables logging of neighbor changes for EIGRP process 1:

```
ipv6 router eigrp 1
 no log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 1:

```
ipv6 router eigrp 1
 log-neighbor-changes
```

Related Commands

Command	Description
log-neighbor- warnings	Enables the logging of EIGRP neighbor warning messages.

managed-config-flag

To verify the advertised managed address configuration parameter, use the **managed-config-flag** command in RA guard policy configuration mode.

managed-config-flag {**on** | **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **managed-config-flag** command enables verification of the advertised managed address configuration parameter (or "M" flag). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables M flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# managed-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

match access-group name

To specify the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class, use the **match access-group name** command in class-map configuration mode. To remove the name of the IPv6 access list, use the **no** form of this command.

match access-group name *ipv6-access-group*
no match access-group name *ipv6-access-group*

Syntax Description

ipv6-access-group	Name of the IPv6 access group. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series routers.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including access control lists (ACLs), protocols, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match access-group name** command specifies an IPv6 named ACL only. The contents of the ACL are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match access-group name** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match dscp**
- **match mpls experimental**
- **match precedence**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Examples

The following example specifies an access list named ipv6acl against whose contents packets will be checked to determine if they belong to the traffic class:

```
class-map ipv6_acl_class
match access-group name ipv6acl
```

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match dscp	Identifies a specific IP DSCP value as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental (EXP) field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity**command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

match identity {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
no match identity {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

Syntax Description

group *group-name*	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the *group-name* argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address *address* [*mask*] [*fvrf*]	Identity that matches the identity of type ID_IPV4_ADDR. • *mask*-- Use to match the range of the address. • *fvrf* --Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
ipv6 *ipv6-address*	Identity that matches the identity of type ID_IPV6_ADDR.
host *host-name*	Identity that matches an identity of the type ID_FQDN.
host domain *domain-name*	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user *user-fqdn*	Identity that matches the FQDN.
user domain *domain-name*	Identity that matches the identities of the type ID_USER_FQDN. When the **user domain** keyword is present, all users having identities of the type ID_USER_FQDN and ending with "*domain-name*" will be matched.

Command Default

No default behavior or values

Command Modes

ISAKMP
profile configuration (conf-isa-prof)

Command History

Release	**Modification**
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and *ipv6-address a*rgument were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

There must be at least one **match identity**command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples

The following example shows that the **match identity**command is configured:

```
crypto isakmp profile vpnprofile
 match identity group vpngroup
 match identity address 10.53.11.1
 match identity host domain example.com
 match identity host server.example.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

match ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}
no match ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY
match ipv6 {**dscp** | **precedence** | **protocol** | **tos**}
no match ipv6 {**dscp** | **precedence** | **protocol** | **tos**}

Cisco IOS XE Release 3.2SE
match ipv6 {**protocol** | **traffic-class** | **version**}
no match ipv6 {**protocol** | **traffic-class** | **version**}

Syntax Description

dscp	Configures the IPv6 differentiated services code point DSCP (part of type of service (ToS)) as a key field.
flow-label	Configures the IPv6 flow label as a key field.
next-header	Configures the IPv6 next header as a key field.
payload-length	Configures the IPv6 payload length as a key field.
precedence	Configures the IPv6 precedence (part of ToS) as a key field.
protocol	Configures the IPv6 protocol as a key field.
tos	Configures the IPv6 ToS as a key field.
traffic-class	Configures the IPv6 traffic class as a key field.
version	Configures the IPv6 version from IPv6 header as a key field.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flexible Netflow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. Support for this command was implemented on the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Release	Modification
12.2(50)SY	This command was modified. The **flow-label**, **next-header**, **payload-length,traffic-class**, and **version** keywords were removed.
15.2(2)T	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.5S	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.2SE	This command was modified. The **dscp**, **flow-label**, **next-header**, **payload-length**, and **precedence** keywords were removed.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Note Some of the keywords of the **match ipv6** command are documented as separate commands. All of the keywords for the **match ipv6** command that are documented separately start with **match ipv6**. For example, for information about configuring the IPv6 hop limit as a key field for a flow record, refer to the **match ipv6 hop-limit** command.

Examples

The following example configures the IPv6 DSCP field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

The following example configures the IPv6 DSCP field as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 access-list

To verify the sender's IPv6 address in inspected messages from the authorized prefix list, use the **match ipv6 access-list** command in RA guard policy configuration mode.

match ipv6 access-list *ipv6-access-list-name*

Syntax Description

ipv6-access-list-name	The IPv6 access list to be matched.

Command Default

Senders' IPv6 addresses are not verified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **match ipv6 access-list** command enables verification of the sender's IPv6 address in inspected messages from the configured authorized router source access list. If the **match ipv6 access-list** command is not configured, this authorization is bypassed.

An access list is configured using the **ipv6 access-list** command. For instance, to authorize the router with link-local address FE80::A8BB:CCFF:FE01:F700 only, define the following IPv6 access list:

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any
```

Note The access list is used here as a convenient way to define several explicit router sources, but it should not be considered to be a port-based access list (PACL). The **match ipv6 access-list** command verifies the IPv6 source address of the router messages, so specifying a destination in the access list is meaningless and the destination of the access control list (ACL) entry should always be "any." If a destination is specified in the access list, then matching will fail.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and matches the IPv6 addresses in the access list named list1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ipv6 access-list list1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.

match ipv6 address

To distribute IPv6 routes that have a prefix permitted by a prefix list or to specify an IPv6 access list to be used to match packets for policy-based routing (PBR) for IPv6, use the **match ipv6 address** command in route-map configuration mode. To remove the **match ipv6 address** entry, use the **no** form of this command.

match ipv6 address {**prefix-list** *prefix-list-nameaccess-list-name*}
no match ipv6 address

Syntax Description

prefix-list *prefix-list-name*	Specifies the name of an IPv6 prefix list.
access-list-name	Name of the IPv6 access list. Names cannot contain a space or quotation mark or begin with a numeric.

Command Default

No routes are distributed based on the destination network number or an access list.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(7)T	This command was modified. The *access-list-name* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXI4	This command was modified. The **prefix-list** *prefix-list-name* keyword-argument pair argument is not supported in Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **route-map** command and the **match** and **set** commands to define the conditions for redistributing routes from one routing protocol to another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, which are the particular redistribution actions to be performed if the criteria enforced by the **match** commands are met.

The **match ipv6 address** command can be used to specify either an access list or a prefix list. When using PBR, you must use the *access-list-name* argument; the **prefix-list** *prefix-list-name* keyword-argument pair argument will not work.

Examples

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```

In the following example, IPv6 routes that have addresses specified by an access list named marketing are matched:

```
Device(config)# route-map
Device(config-route-map)# match ipv6 address marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match ipv6 next-hop	Distributes IPv6 routes that have a next-hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match length	Bases policy routing on the Level 3 length of a packet.
match metric	Redistributes routes with the specified metric.
match route-type	Redistributes routes of the specified type.
route-map	Defines conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

Command	Description
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 destination

To configure the IPv6 destination address as a key field for a flow record, use the **match ipv6 destination** command in Flexible Netflow flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the **no** form of this command.

match ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}
no match ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY
match ipv6 destination address
no match ipv6 destination address

Cisco IOS XE Release 3.2SE
match ipv6 destination address
no match ipv6 destination address

Syntax Description

address	Configures the IPv6 destination address as a key field.
mask	Configures the mask for the IPv6 destination address as a key field.
prefix	Configures the prefix for the IPv6 destination address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 128.

Command Default

The IPv6 destination address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. Support for this command was implemented on the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **mask**, **prefix**, and **minimum-mask** keywords were removed.
15.2(2)T	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.5S	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.2SE	This command was modified. The **mask**, **prefix**, and **minimum-mask** keywords were removed.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a 16-bit IPv6 destination address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination prefix minimum-mask 16
```

The following example specifies a 16-bit IPv6 destination address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

The following example configures a 16-bit IPv6 destination address mask as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 extension map

To configure the bitmap of the IPv6 extension header map as a key field for a flow record, use the **match ipv6 extension map** command in flow record configuration mode. To disable the use of the IPv6 bitmap of the IPv6 extension header map as a key field for a flow record, use the **no** form of this command.

match ipv6 extension map
no match ipv6 extension map

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the bitmap of the IPv6 extension header map as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Bitmap of the IPv6 Extension Header Map

The bitmap of IPv6 extension header map is made up of 32 bits.

```
   0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
| Res | FRA1| RH  | FRA0| UNK | Res | HOP | DST |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

```
    8     9    10    11    12    13    14    15
+-----+-----+-----+-----+-----+-----+----+-----+
| PAY | AH  | ESP |         Reserved           |
+-----+-----+-----+-----+-----+-----+----+-----+
   16    17    18    19    20    21    22    23
+-----+-----+-----+-----+-----+-----+----+-----+
|                  Reserved                    |
+-----+-----+-----+-----+-----+-----+----+-----+
   24    25    26    27    28    29    30    31
+-----+-----+-----+-----+-----+-----+----+-----+
|                  Reserved                    |
+-----+-----+-----+-----+-----+-----+----+-----+
0  Res  Reserved
1  FRA1 Fragmentation header - not first fragment
2  RH   Routing header
3  FRA0 Fragment header - first fragment
4  UNK  Unknown Layer 4 header
         (compressed, encrypted, not supported)
5  Res  Reserved
6  HOP  Hop-by-hop option header
7  DST  Destination option header
8  PAY Payload compression header
9  AH  Authentication Header
10 ESP Encrypted security payload
11 to 31 Reserved
```

For more information on IPv6 headers, refer to RFC 2460 *Internet Protocol, Version 6 (IPv6)* at the following URL: http://www.ietf.org/rfc/rfc2460.txt .

Examples

The following example configures the IPv6 bitmap of the IPv6 extension header map of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 extension map
```

Cisco Performance Monitor in Cisco IOS Release 15.2(2)T and XE 3.5S

The following example configures the IPv6 bitmap of the IPv6 extension header map of the packets in the flow as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 extension map
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 fragmentation

To configure one or more of the IPv6 fragmentation fields as a key field for a flow record, use the **match ipv6 fragmentation** command in flow record configuration mode. To disable the use of the IPv6 fragmentation field as a key field for a flow record, use the **no** form of this command.

match IPv6 fragmentation {**flags** | **id** | **offset**}
no match IPv6 fragmentation {**flags** | **id** | **offset**}

Syntax Description

flags	Configures the IPv6 fragmentation flags as a key field.
id	Configures the IPv6 fragmentation ID as a key field.
offset	Configures the IPv6 fragmentation offset value as a key field.

Command Default

The IPv6 fragmentation field is not configured as a key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv6 fragmentation flags a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation flags
```

The following example configures the IPv6 offset value a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation offset
```

Cisco Performance Monitor in Cisco IOS Release 15.2(2)T and XE 3.5S

The following example configures the IPv6 offset value as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 fragmentation offset
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a flow record, use the **match ipv6 hop-limit** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the **no** form of this command.

match ipv6 hop-limit
no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. Support for this command was implemented on the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.5S	This command was modified. Support for the Cisco Performance Monitor was added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the hop limit of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

The following example configures the hop limit of the packets in the flow as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 length

To configure one or more of the IPv6 length fields as a key field for a flow record, use the **match ipv6 length** command in flow record configuration mode. To disable the use of the IPv6 length field as a key field for a flow record, use the **no** form of this command.

match ipv6 length {**header** | **payload** | **total**}
no match ipv6 length {**header** | **payload** | **total**}

Syntax Description

header	Configures the length in bytes of the IPv6 header, not including any extension headers as a key field.
payload	Configures the length in bytes of the IPv6 payload, including any extension header as a key field.
total	Configures the total length in bytes of the IPv6 header and payload as a key field.

Command Default

The IPv6 length field is not configured as a key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the length of the IPv6 header in bytes, not including any extension headers, as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 length header
```

Cisco Performance Monitor in Cisco IOS Release 15.2(2)T and XE 3.5S

The following example configures the length of the IPv6 header in bytes, not including any extension headers, as a key field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 length header
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record, and enters Performance Monitor flow record configuration mode.

match ipv6 next-hop

To distribute IPv6 routes that have a next hop prefix permitted by a prefix list, use the **match ipv6 next-hop** command in route-map configuration mode. To remove the **match ipv6 next-hop** entry, use the **no** form of this command.

match ipv6 next-hop prefix-list *prefix-list-name*
no match ipv6 next-hop

Syntax Description

prefix-list *prefix-list-name*	Name of an IPv6 prefix list.

Command Default

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **match ipv6 next-hop**command is similar to the **match ip next-hop**command, except that it is IPv6-specific.

Use the route-map command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*--the conditions under which redistribution is allowed for the current route-mapcommand. The **set** commands specify the *set actions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Note A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have a next hop IPv6 address passed by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 next-hop prefix-list marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ipv6 route-source

To distribute IPv6 routes that have been advertised by routers at an address specified by a prefix list, use the **match ipv6 route-source** command in route-map configuration mode. To remove the **match ipv6 route-source** entry, use the **no** form of this command.

match ipv6 route-source prefix-list *prefix-list-name*
no match ipv6 route-source

Syntax Description

prefix-list *prefix-list-name*	Name of an IPv6 prefix list.

Command Default

No filtering on route source.

Command Modes

Route-map configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **match ipv6 route-source**command is similar to the **match ip route-source** command, except that it is IPv6-specific.

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*--the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions*given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

There are situations in which the next hop for a route and the source networking device address are not the same.

Note A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have been advertised by networking devices at the addresses specified by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 route-source prefix-list marketing
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match metric	Redistributes routes with the metric specified.
match route-type	Redistributes routes of the specified type.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP community attribute.
set level	Indicates where to import routes.
set local preference	Specifies a preference value for the autonomous system path.
set metric	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match ra prefix-list

To verify the advertised prefixes in inspected messages from the authorized prefix list, use the **match ra prefix-list** command in RA guard policy configuration mode.

match ra prefix-list *ipv6-prefix-list-name*

Syntax Description

ipv6-prefix-list-name	The IPv6 prefix list to be matched.

Command Default

Advertised prefixes are not verified.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **match ra prefix-list** command enables verification of the advertised prefixes in inspected messages from the configured authorized prefix list. Use the **ipv6 prefix-list** command to configure an IPv6 prefix list. For instance, to authorize the 2001:101::/64 prefixes and deny the 2001:100::/64 prefixes, define the following IPv6 prefix list:

```
Router(config)# ipv6 prefix-list listname1 deny 2001:0DB8:101:/64
Router(config)# ipv6 prefix-list listname1 permit 2001:0DB8:100::/64
```

Examples

The following example shows how the command defines an router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and verifies the advertised prefixes in listname1:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ra prefix-list listname1
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.

maximum-paths (IPv6)

To control the maximum number of equal-cost routes that a process for IPv6 Border Gateway Protocol (BGP), a process for IPv6 Intermediate System-to-Intermediate System (IS-IS), a process for IPv6 Routing Information Protocol (RIP), a process for Open Shortest Path First (OSPF) for IPv6, or a process for Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing can support, use the **maximum-paths**command in address family configuration or router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*
no maximum-paths

Syntax Description

number-paths	Maximum number of equal-cost paths to a destination learned via IPv6 BGP, IS-IS, RIP, OSPF, or EIGRP installed in the IPv6 routing table, in the range from 1 to 64.

Command Default

The default for BGP is 1 path, the default for IS-IS and RIP is 4 paths, and the default for OSPF for IPv6 is 16 paths .

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S and support for IPv6 RIP was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	Support for IPv6 OSPF was added.
12.4(6)T	Support for EIGRP for IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To configure the **maximum-paths**command for IPv6 BGP and IS-IS, enter address family configuration mode.

Examples

The following example shows a maximum of three paths to an external destination for the IPv6 BGP autonomous system 65000, and a maximum of two paths to an IPv6 internal BGP destination being configured:

```
Router(config)# router bgp 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 3
Router(config-router-af)# maximum-paths ibgp 2
```

The following example shows a maximum of two paths to a destination for the IPv6 IS-IS routing process named area01 being configured:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 2
```

The following example shows a maximum of one path to a destination for the IPv6 RIP routing process named one being configured:

```
Router(config)# ipv6 router rip one
Router(config-router-rip)# maximum-paths 1
```

The following example shows a maximum of four paths to a destination for an IPv6 OSPF routing process:

```
Router(config) ipv6 router ospf 1
Router(config-router)# maximum-paths 4
```

The following example shows a maximum of two paths to a destination for an EIGRP for IPv6 routing process:

```
Router(config) ipv6 router eigrp 1
Router(config-router)# maximum-paths 2
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.
ipv6 router rip	Configures an IPv6 RIP routing process.
router bgp	Configures the BGP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

maximum-paths (OSPFv3)

To control the maximum number of equal-cost routes that a process for Open Shortest Path First version 3 (OSPFv3) routing can support, use the **maximum-paths**command in IPv6 or IPv4 address family configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*
no maximum-paths

Syntax Description

number-paths	Maximum number of equal-cost paths to a destination learned through OSPFv3. The range is from 1 through 64.

Command Default

16 equal-cost paths

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to control the maximum number of equal-cost routes that a process for OSPFv3 routing can support.

Examples

The following example shows how to configure a maximum of four paths to a destination for an OSPFv3 routing process:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# maximum-paths 4
```

mls ipv6 acl compress address unicast

To enable the compression of compressible IPv6 addresses, use the **mls ipv6 acl compress address unicast** command in global configuration mode. To disable the compression of compressible IPv6 addresses, use the **no** form of this command.

mls ipv6 acl compress address unicast
no mls ipv6 acl compress address unicast

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note Do not enable the compression mode if you have noncompressible address types in your network. Compressible address types and the address compression method are listed in the table below.

Table 7: Compressible Address Types and Methods

Address Type	Compression Method
EUI-64 based on MAC address	This address is compressed by removing 16 bits from bit locations [39:24]. No information is lost when the hardware compresses these addresses.
Embedded IPv4 address	This address is compressed by removing the upper 16 bits. No information is lost when the hardware compresses these addresses.
Link Local	These addresses are compressed by removing the zeros in bits [95:80] and are identified using the same packet type as the embedded IPv4 address. No information is lost when the hardware compresses these addresses.

Address Type	Compression Method
Other	If the IPv6 address does not fall into any of the categories, it is classified as Other. If the IPv6 address is classified as Other, the following occurs: • If the compress mode is on, the IPv6 address is compressed similarly to the EUI-64 compression method (removal of bits [39:24]) to allow for the Layer 4 port information to be used as part of the key used to look up the quality of service (QoS) ternary content addressable memory (TCAM), but Layer 3 information is lost. • If the global compression mode is off, the entire 128 bits of the IPv6 address are used. The Layer 4 port information cannot be included in the key to look up the QoS TCAM because of the size constraints on the IPv6 lookup key.

Examples

This example shows how to turn on the compression of compressible IPv6 addresses:

```
Router(config)#
mls ipv6 acl compress address unicast
```

This example shows how to turn off the compression of compressible IPv6 addresses:

```
Router(config)#
no mls ipv6 acl compress address unicast
```

Related Commands

Command	Description
show fm ipv6 traffic-filter	Displays the IPv6 information.
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 acl source

To deny all IPv6 packets from a source-specific address, use the **mls ipv6 acl source**command in global configuration mode. To accept all IPv6 packets from a source-specific address, use the **no** form of this command.

mls ipv6 acl source {**loopback** | **multicast**}
no mls ipv6 acl source {**loopback** | **multicast**}

Syntax Description

loopback	Denies all IPv6 packets with a source loopback address .
multicast	Denies all IPv6 packets with a source multicast address.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17b)SXA	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to deny all IPv6 packets with a source loopback address:

```
Router(config)#
mls ipv6 acl source loopback
```

This example shows how to deny all IPv6 packets with a source multicast address:

```
Router(config)#
no mls ipv6 acl source multicast
```

Related Commands

Command	Description
show mls netflow ipv6	Displays configuration information about the NetFlow hardware.

mls ipv6 slb search wildcard rp

To specify the behavior of Server Load Balancing (SLB) wildcard searches by the route processor (RP), use the **mls ipv6 slb search wildcard rp** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls ipv6 slb search wildcard rp
no mls ipv6 slb search wildcard rp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.2(4)S	This command was introduced on the Cisco 7600 Series devices.

Usage Guidelines

This command is supported for Cisco 7600 Series devices only.

Examples

The following example shows how to configure the SLB wildcard searches:

```
Router(config)# mls ipv6 slb search wildcard rp
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall by IP address farm and enters firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.

mls ipv6 vrf

To enable IPv6 globally in a virtual routing and forwarding (VRF) instance, use the mls ipv6 vrf command in global configuration mode. To remove this functionality, use the no form of the command.

mls ipv6 vrf
no mls ipv6 vrf

Syntax Description

This command has no arguments or keywords.

Command Default

VRFs are supported only for IPv4 addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI and implemented on the Catalyst 6500 series switches.

Usage Guidelines

You must enable the mls ipv6 vrf command in global configuration mode in order to enable IPv6 in a VRF. If this command is not used, a VRF is supported only for the IPv4 address family.

Configuring the mls ipv6 vrf command makes the router reserve the lower 255 hardware IDs for IPv6 regardless of whether IPv6 is enabled. Other applications that make use of these hardware IDs then cannot use that space.

To remove the **mls ipv6 vrf** command from the running configuration, the user needs to remove all IPv6 VRFs from the router and reload the system.

Examples

The following example shows how to enable IPv6 in a VRF globally:

```
Router(config)# mls ipv6 vrf
```

Related Commands

Command	Description
vrf definition	Configure a VRF routing table instance and enters VRF configuration mode.
show running-config vrf	Displays the subset of the running configuration of a router that is linked to a specific VRF instance or to all VRFs configured on the router.

mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6**command in global configuration mode. To disable the rate limiters, use the **no** form of this command.

```
mls rate-limit multicast ipv6 {connected pps [packets-in-burst]|
rate-limiter-name share {auto|target-rate-limiter}}
```

no mls rate-limit multicast ipv6 {**connected***rate-limiter-name*}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source ; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
rate-limiter-name	Rate-limiter name; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the "Usage Guidelines" section for additional information.
share	Specifies the sharing policy for IPv6 rate limiters; see the "Usage Guidelines" section for additional information.
auto	Decides the sharing policy automatically.
target-rate-limiter	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the "Usage Guidelines" section for additional information.

Command Default

If the *burst* is not set, a default of **100** is programmed for multicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *rate-limiter-name*argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter*argument must be a rate limiter that is programmed in the hardware and must be the first rate limiterprogrammed for its group.

The table below lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 8: IPv6 Rate Limiters

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class--Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- Static sharing of a rate limiter with another preconfigured rate limiter--When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-cntl** rate limiter with the **default-drop** target rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters--If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mode dad-proxy

To enable duplicate address detection (DAD) proxy mode for IPv6 Neighbor Discovery (ND) suppress, use the **mode dad-proxy** command in ND suppress policy configuration mode. To disable this feature, use the **no** form of this command.

mode dad-proxy

Syntax Description

This command has no arguments or keywords.

Command Default

All multicast neighbor solicitation (NS) messages are suppressed.

Command Modes

ND suppress policy configuration mode (config-nd-suppress)

Command History

Release	Modification
15.1(2)SG	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The IPv6 Dad proxy feature responds on behalf of the address's owner when an address is already in use. Use the **mode dad-proxy** command to enable IPv6 DAD proxy when using IPv6 ND suppress. If your device does not support IPv6 multicast suppress, you can enable IPv6 DAD proxy by entering the **ipv6 nd dad-proxy** command in global configuration mode.

Examples

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)# mode dad-proxy
```

Related Commands

Command	Description
ipv6 nd dad-proxy	Enables the IPv6 ND DAD proxy feature on the device.
ipv6 nd suppress policy	Enables IPv6 ND multicast suppress and enters ND suppress policy configuration mode.

monitor event ipv6 static

To monitor the operation of the IPv6 static and IPv6 static Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors using event trace, use the **monitor event ipv6 static** command in privileged EXEC mode. To disable monitoring, use the **no** form of the command.

monitor event ipv6 static
no monitor event ipv6 static

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 static and IPv6 static BFD neighbors are not monitored.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1.0	This command was introduced.
15.1(2)T	This command was modified. It was integrated into Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **monitor event ipv6 static** command to monitor the operation of IPv6 static and IPv6 static BFDv6 neighbors and collect data.

Examples

The following example enables event trace to monitor BFDv6 operation:

```
Router# monitor event ipv6 static
```

Related Commands

Command	Description
debug ipv6 static	Enables BFDv6 debugging.
show ipv6 static	Displays the current contents of the IPv6 routing table.

monitor event-trace cef ipv6 (global)

To configure event tracing for Cisco Express Forwarding IPv6 events, use the **monitor event-trace cef ipv6**command in global configuration mode. To disable event tracing for Cisco Express Forwarding, use the **no** form of this command.

monitor event-trace cef ipv6 {**disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **math** {**global***ipv6-address/n*} | **size** *number* | **stacktrace** [*depth*] | **vrf** *vrf-name* [{**distribution** | **match**{**global***ipv6-address/n*}}]}
no monitor event-trace cef ipv6 {**disable** | **distribution** | **dump-file** *dump-file-name* | **enable** | **match** | **size** | **stacktrace** [*depth*] | **vrf**}

Syntax Description

disable	Turns off event tracing for Cisco Express Forwarding IPv6 events.
distribution	Logs events related to the distribution of Cisco Express Forwarding Forwarding Information Base (FIB) tables to the line cards.
dump-file *dump-file-name*	Specifies the file to which event trace messages are written from memory on the networking device. The maximum length of the filename (path and filename) is 100 characters, and the path can point to flash memory on the networking device or to a TFTP or FTP server.
enable	Turns on event tracing for Cisco Express Forwarding IPv6 events if it had been enabled with the **monitor event-trace cef ipv6**command.
match	Turns on event tracing for Cisco Express Forwarding IPv6 that matches global events or events that match a specific network address.
global	Specifies global events.
ipv6-address / *n*	Specifies an IPv6 address. This address must be in the form documented in RFC 2373: the address is specified in hexadecimals using 16-bit values between colons. The slash followed by a number (/ *n*) indicates the number of bits that do not change. Range: 0 to 128.
size *number*	Sets the number of messages that can be written to memory for a single instance of a trace. Range: 1 to 65536. **Note** Some Cisco IOS software subsystem components set the size by default. To display the size parameter, use the **show monitor event-trace cef parameters** command. When the number of event trace messages in memory exceeds the configured size, new messages will begin to overwrite the older messages in the file.
stacktrace	Enables the stack trace at tracepoints.
depth	(Optional) Specifies the depth of the stack trace stored. Range: 1 to 16.
vrf *vrf-name*	Turns on event tracing for a Cisco Express Forwarding IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) table. The *vrf-name* argument specifies the name of the VRF.

Command Default

Event tracing for Cisco Express Forwarding IPv6 events is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use the **monitor event-trace cef ipv6**command to enable or disable event tracing for Cisco Express Forwarding IPv6 events.

The Cisco IOS software allows Cisco Express Forwarding to define whether support for event tracing is enabled or disabled by default. The command interface for event tracing allows you to change the default value in one of two ways: using the **monitor event-trace cef ipv6**command in privileged EXEC mode or using the **monitor event-trace cef ipv6**command in global configuration mode.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace cef ipv6**command for each instance of a trace.

To determine whether event tracing is enabled by default for Cisco Express Forwarding IPv6 events, use the **show monitor event-trace cef ipv6**command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for Cisco Express Forwarding IPv6 events and configure the buffer size to 10000 messages.

```
Router(config)# monitor event-trace cef ipv6 enable
Router(config)# monitor event-trace cef ipv6 size 10000
```

Related Commands

Command	Description
monitor event-trace cef (EXEC)	Monitors and controls the event trace function for Cisco Express Forwarding.
monitor event-trace cef (global)	Configures event tracing for Cisco Express Forwarding.
monitor event-trace cef ipv4 (global)	Configures event tracing for Cisco Express Forwarding IPv4 events.

Command	Description
show monitor event-trace cef	Displays event trace messages for Cisco Express Forwarding.
show monitor event-trace cef events	Displays event trace messages for Cisco Express Forwarding events.
show monitor event-trace cef interface	Displays event trace messages for Cisco Express Forwarding interface events.
show monitor event-trace cef ipv4	Displays event trace messages for Cisco Express Forwarding IPv4 events.
show monitor event-trace cef ipv6	Displays event trace messages for Cisco Express Forwarding IPv6 events.

monitor event-trace ipv6 spd

To monitor Selective Packet Discard (SPD) state transition events, use the monitor event-trace ipv6 spd command in privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor event-trace ipv6 spd
no monitor event-trace ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **monitor event-trace ipv6 spd** command to check SPD state transition events.

multi-topology

To enable multitopology Intermediate System-to-Intermediate System (IS-IS) for IPv6, use the **m ulti-topology** command in address family configuration mode. To disable multitopology IS-IS for IPv6, use the **no** form of this command.

multi-topology [**transition**]
no multi-topology

Syntax Description

transition	(Optional) Allows an IS-IS IPv6 user to continue to use single shortest path first (SPF) mode while upgrading to multitopology IS-IS for IPv6.

Command Default

Multitopology IS-IS is disabled by default.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

By default, the router runs IS-IS IPv6 in single SPF mode. The **multi-topology** command enables multitopology IS-IS for IPv6.

The optional transition keyword can be used to migrate from IS-IS IPv6 single SPF mode to multitopology IS-IS IPv6. When transition mode is enabled, the router advertises both multitopology type, length, and value (TLV) objects and single-SPF-mode IS-IS IPv6 TLVs, but the SPF is computed using the single-SPF-mode IS-IS IPv6 TLV. This action has the side effect of increasing the link-state packet (LSP) size.

Examples

The following example enables multitopology IS-IS for IPv6:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# multi-topology
```

IPv6 Commands: n to re

nai (proxy mobile IPv6)

To configure the Network Access Identifier (NAI) for the mobile node (MN) within the PMIPV6 domain, use the **nai** command in PMIPV6 domain configuration mode. To disable the NAI configuration, use the **no** form of this command.

nai [*user*] *@realm*
no nai [*user*] *@realm*

Syntax Description

user@realm	Fully qualified specific user address and realm. The @ symbol is required.
@realm	Any user address at a specific realm. The @ symbol is required.

Command Default

NAI for the MN is not specified.

Command Modes

PMIPV6 domain configuration (config-ipv6-pmipv6-domain)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following example shows how to configure the NAI within the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example@example.com
Device(config-ipv6-pmipv6-domain-mn)#
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg**command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-nameipv6-address*} **override-capability-neg**
no neighbor {*peer-group-nameipv6-address*} **override-capability-neg**

Syntax Description

peer-group-name	Name of a BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg**command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg**command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]
no neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.
send-label	Sends Network Layer Reachability Information (NLRI) and MPLS labels to this peer.
explicit-null	(Optional) Advertises the Explicit Null label.

Command Default

BGP routers distribute only BGP routes.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *ipv6-address* argument was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **neighbor send-label** command enables a router to use BGP to distribute MPLS labels along with IPv4 routes to a peer router. You must issue this command on both the local and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the BGP session flaps immediately after the command is issued.
- In router configuration mode, only IPv4 addresses are distributed.

Use the **neighbor send-label** command in address family configuration mode, to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 traffic forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS software installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in autonomous system 65000 to send MPLS labels with BGP routes to the neighboring BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighboring BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
mpls ipv6 source-interface	Specifies an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over an MPLS network.

neighbor translate-update

To enable customer-edge (CE) devices, which are not capable of multicast BGP (mBGP) routing, to participate in a multicast session, use the **neighbor translate-update** command in address-family configuration mode. To disable mBGP routing on CE devices, use the **no** form of the command.

neighbor {*ipv4-address ipv6-address*} **translate-update multicast** [**unicast**]
no neighbor {*ipv4-address ipv6-address*} **translate-update multicast** [**unicast**]

Syntax Description

ipv4-address	Specifies the multicast IPv4 address for the BGP neighbor.
ipv6-address	Specifies the multicast IPv6 address for the BGP neighbor.
multicast	Specifies multicast address prefixes.
unicast	(Optional) Specifies unicast address prefixes.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.4(1)S	This command was modified. Support for translate-update was extended to VRF address-families.
Cisco IOS XE Release 3.11S	This command was modified. Support for translate-update was extended to VRF address-families.

Usage Guidelines

The **translate-update** keyword in the neighbor command enables CE devices, which cannot send BGP Reverse Path Forwarding (RPF) multicast routes, to advertise its routes to multicast VRF-Lite and multicast VPN (mVPN) for VPNv4 and VPNv6 neighbors. These routes are also advertised through IPv6 over IPv4 tunnel. The **translate-update** keyword is configured on the provider-edge (PE) devices for multicast routing to neighbor CE devices using the **address-family ipv4 vrf** or the **address-family ipv6 vrf** command. The PE devices translate the updates from unicast to multicast on CE devices and put them in the BGP VRF routing table of the PE devices, as multicast updates, for processing. If the optional keyword **unicast** is also configured, the updates that are not translated to multicast are also placed in the unicast queue of the PE devices and populate the unicast BGP VRF table. The translation from unicast to multicast occurs from CE devices to PE devices only. Prefixes are only advertised from CE devices to the multicast neighbors of the PE devices.

Prior to configuring the translate-update feature, you must enable multicast VRF on the PE devices, along with an active VRF session with the CE devices.

Examples

The following example shows how to configure the translate-update feature for an IPv4 VRF address-family named v1 and BGP neighbor n2:

Note Peer-template configuration for BGP neighbor is not supported for this feature due to conflicts with the earlier versions of Cisco software.

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 vrf v1
Device(config-router-af)# neighbor n2 peer-group
Device(config-router-af)# neighbor n2 remote-as 4
Device(config-router-af)# neighbor 10.1.1.1 peer-group n2
Device(config-router-af)# neighbor 10.1.1.1 activate
Device(config-router-af)# neighbor 10.1.1.1 translate-update multicast unicast
Device(config-router-af)# end
```

The following is sample output from the **show bgp vpnv4 multicast vrf** command. If the “State/PfxRcd” field displays “NoNeg”, it indicates that the neighbor has a translate-update session:

```
Device# show bgp vpnv4 multicast vrf v1 summary

BGP router identifier 10.1.3.1, local AS number 65000
BGP table version is 8, main routing table version 8
7 network entries using 1792 bytes of memory
8 path entries using 960 bytes of memory
5/3 BGP path/bestpath attribute entries using 1280 bytes of memory
3 BGP AS-PATH entries using 88 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4168 total bytes of memory
BGP activity 23/2 prefixes, 33/9 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.1        4            4       5      10        1    0    0 00:01:10 (NoNeg)

10.1.3.2        4            2      12      10        8    0    0 00:01:33
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv6 address prefixes.

Command	Description
neighbor peer-group	Creates a BGP or multiprotocol BGP peer group.
neighbor remote-as	Adds an entry to a BGP or multiprotocol BGP neighbor table.
neighbor activate	Enables exchange of information with a BGP neighbor.
show bgp vpnv4 multicast	Displays Virtual Private Network Version 4 (VPNv4) multicast entries in a BGP table.

network (IPv6)

To configure the network source of the next hop to be used by the PE VPN, use the network command in router configuration mode. To disable the source, use the **no** form of this command.

network *ipv6-address/prefix-length*
no network *ipv6-address/prefix-length*

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Next-hop network sources are not configured.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The *ipv6-address* argument in this command configures the IPv6 network number.

Examples

The following example places the router in address family configuration mode and configures the network source to be used as the next hop:

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.

nis address

To specify the network information service (NIS) address of an IPv6 server to be sent to the client, use the **nis address** command in DHCP for IPv6 pool configuration mode. To remove the NIS address, use the **no** form of this command.

nis address *ipv6-address*
no nis address *ipv6-address*

Syntax Description

ipv6-address	The NIS address of an IPv6 server to be sent to the client.

Command Default

No NIS address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS server option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server’s preference.

The NIS server option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS address of an IPv6 server:

```
nis address 23::1
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis domain-name	Enables a server to convey a client’s NIS domain name information to the client.

nis domain-name

To enable a server to convey a client's network information service (NIS) domain name information to the client, use the **nis domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nis domain-name *domain-name*
no nis domain-name *domain-name*

Syntax Description

domain-name	The domain name of an IPv6 server to be sent to the client.

Command Default

No NIS domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client. Use the **nis domain-name** command to specify the client's NIS domain name that the server sends to the client.

The NIS domain name option code is 29. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS domain name of a client:

```
nis domain-name cisco1.com
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.

nisp address

To specify the network information service plus (NIS+) address of an IPv6 server to be sent to the client, use the **nisp address** command in DHCP for IPv6 pool configuration mode. To remove the NIS+ address, use the **no** form of the command.

nisp address *ipv6-address*
no nisp address *ipv6-address*

Syntax Description

ipv6-address	The NIS+ address of an IPv6 server to be sent to the client.

Command Default

No NIS+ address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS+ address of an IPv6 server:

```
nisp address 33::1
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ servers option to a DHCP for IPv6 client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

nisp domain-name

To enable an IPv6 server to convey a client's network information service plus (NIS+) domain name information to the client, use the **nisp domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nisp domain-name *domain-name*
no nisp domain-name *domain-name*

Syntax Description

domain-name	The NIS+ domain name of an IPv6 server to be sent to the client.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides a NIS+ domain name for the client. Use the **nisp domain-name** command to enable a server to send the client its NIS+ domain name information.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS+ domain name of a client:

```
nisp domain-name cisco1.com
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.

ospfv3 area

To enable Open Shortest Path First version 3 (OSPFv3) on an interface with the IPv4 or IPv6 address family (AF), use the **ospfv3 area** command in interface configuration mode. To disable OSPFv3 routing for interfaces defined, use the **no** form of this command.

ospfv3 *process-id* {**ipv4** | **ipv6**}**area** *area-ID* [**instance** *instance-id*]
no ospfv3 *process-id* {**ipv4** | **ipv6**}**area** *area-ID*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
ipv4	IPv4 address family.
ipv6	IPv6 address family.
area-id	Area that is to be associated with the OSPFv3 interface.
instance *instance-id*	(Optional) Instance identifier. • When the **ipv4** keyword is used, the *instance-id* argument can be a value from 64 through 95. The default is 64. • When the **ipv6** keyword is used, the *instance-id* argument can be a value from 0 through 31. The default is 0.

Command Default

OSPFv3 is not enabled on the interface. The default instance ID for IPv4 is 64. The default instance ID for IPv6 is 0.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 area**command to enable OSPFv3 on an interface. This command enables you to configure two OSPFv3 instances on an interface-one IPv6 AF instance, and one IPv4 AF instance. You can configure only one process for each AF per interface.

Before you enable OSPFv3 on an interface using the **ospfv3 area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

When the **ospfv3 area**command is configured for the IPv6 AF, it overwrites the **ipv6 ospf area** configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

Examples

The following example enables OSPFv3 for the IPv4 AF on an interface:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 1 area 1 ipv4
```

ospfv3 authentication

To specify the authentication type for an Open Shortest Path First version 3 (OSPFv3) instance, use the **ospfv3 authentication**command in interface configuration mode. To remove this instance, use the **no** form of this command.

{**ospfv3 authentication ipsec** *spi* {**md5** | **sha1**} *key-encryption-type key* | **null**}
{**no ospfv3 authentication ipsec** *spi* {**md5** | **sha1**} *key-encryption-type key* | **null**}

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
md5	Enables message digest 5 (MD5) authentication.
sha1	Enables Secure Hash Algorithm 1 (SHA-1) authentication.
key-encryption-type	One of the following values can be entered: • **0** --The key is not encrypted. • **7** --The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
null	Used to override area authentication.

Command Default

No authentication is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 authentication** command to specify the OSPFv3 authentication type on an interface. The **ospfv3 authentication** command cannot be configured per process. If the **ospfv3 authentication** command is used, it affects all OSPFv3 instances.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPsec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **authentication null**command.

Examples

The following example specifies the authentication type for an OSPFv3 instance:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 authentication md5 0 27576134094768132473302031209727
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 bfd

To enable Bidirectional Forwarding Detection (BFD) on an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 bfd** command in interface configuration mode. To remove this instance, use the **no** form of this command.

ospfv3 [*process-id*] **bfd** [**disable**]
no ospfv3 [*process-id*] **bfd**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Disables BFD on the specified interface.

Command Default

BFD support for OSPFv3 is not enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 bfd** command to enable BFD on an interface. When the **ospfv3 bfd** command is entered with a process ID, it applies to that specific process only. This configuration takes precedence if the **ospfv3 bfd** command is enabled with no specified process ID.

If you have used the **bfd all-interfaces** command in router configuration mode to globally configure all OSPFv3 interfaces for an OSPFv3 process to use BFD, you can enter the **bfd** command in interface configuration mode with the **disable** keyword to disable BFD for a specific OSPFv3 interface.

Examples

The following example enables BFD on OSPFv3:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 bfd
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 cost

To explicitly specify the cost of sending a packet on an Open Shortest Path First version 3 (OSPFv3) interface, use the ospfv3 **cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **cost** {*interface-cost* | **dynamic** [**default** *default-link-metric*] | **hysteresis** [*percent* | **threshold** *threshold-value*] | **weight** {**L2-factor** *percent* | **latency** *percent* | **resources** *percent* | **throughput** *percent*}
no ospfv3 [*process-id*] **cost**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
interface-cost	Route cost of this interface. It can be a value in the range from 1 to 65535.
dynamic	Default value on VMI interfaces.
default	(Optional) Default link metric value.
default-link-metric	Specifies the default link metric value on this interface. It can be a value in the range from 0 to 65535.
hysteresis	(Optional) Hysteresis value for link-state advertisement (LSA) dampening.
percent	(Optional) The percentage of c
threshold *threshold-value*	(Optional) Cost change threshold at which hysteresis will be implemented. The threshold range is from 0 to 64k, and the default threshold value is 10k.
weight	(Optional) Amount of impact a variable has on the dynamic cost.
L2-factor *percent*	Quality weight of the Layer 2 link expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
latency *percent*	Latency weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
resources *percent*	Resources weight (such as battery life) of the router at the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.
throughput *percent*	Throughput weight of the Layer 2 link, expressed as a percentage. The *percent* value can be in the range from 0 to 100. The default value is 100.

Command Default

Default cost is based on the bandwidth. Mobile Ad Hoc Network (MANET) interfaces are set to use dynamic costs. Non-MANET networks are set to use static costs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 cost**command to specify the cost of sending a packet on an interface. When the **ospfv3 cost**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf cost**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 cost**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

You can set the metric manually using the **ospfv3 cost** command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as the **ospfv3 cost** command is not used. The link-state metric is advertised as the link cost in the router link advertisement.

The dynamic cost metric used for interfaces is computed based on the Layer 2 (L2) feedback to Layer 3 (L3). For a dynamic cost to have the same cost as a default cost, all parameters must equal zero.

Each Layer 2 feedback can contribute a cost in the range of 0 to 65535. To tune down this cost range, use the optional **weight** keyword in conjunction with the **throughput**, **resources**, **latency**, or **L2-factor** keyword. Each of these weights has a default value of 100% and can be configured in the range from 0 to 100. When 0 is configured for a specific weight, that weight does not contribute to the OSPFv3 cost.

Because cost components can change rapidly, you may need to dampen the amount of changes in order to reduce network-wide churn. Use the optional **hysteresis** keyword with the **threshold** *threshold-value* keyword and argument to set a cost change threshold. Any cost change below this threshold is ignored.

If you enable hysteresis without specifying the mode (percent or threshold), the default mode is threshold, and 10k as the default threshold value.

The higher the threshold or the percent value is set, the larger the change in link quality required to change the OSPFv3 route costs.

Mobile Ad Hoc Networks (MANET)

When the network type is set to MANET, the OSPF cost associated with an interface automatically sets to dynamic. All other network types, keep the interface cost, and you must enter the **ospfv3 cost dynamic** command to change the cost to dynamic.

If you do not specify a default dynamic cost with the **ospfv3 cost dynamic default** command, OSPF uses the interface cost until it receives link metric data.

Examples

The following example sets the interface cost value to 65:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 cost 65
```

The following example shows how to configure OSPFv3 instance 4 to use 30 as the default cost until link metric data arrives from dynamic costing:

```
Router(config)# interface ethernet 0/0
```

```
Router(config-if)# ospfv3 4 cost dynamic default 30
Router(config-if)# exit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 database-filter

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First version 3 (OSPFv3) interface, use the **database-filter**command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ospfv3 [*process-id*] **database-filter** [{**all** | **disable**}]
no ospfv3 database-filter

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
all	(Optional) Filters all LSAs on the OSPFv3 interface.
disable	(Optional) Disables the LSA filter on the OSPFv3 interface.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 database-filter**command to filter outgoing LSAs to an OSPFv3 interface. When the **ospfv3 database-filter**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf database-filter** configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 database-filter** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Examples

The following example prevents flooding of OSPFv3 LSAs to networks reachable through Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 database-filter
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the ospfv3 **dead-interval**command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **dead-interval** *seconds*
no **ospfv3** [*process-id*] **dead-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network. The value can be from 1 through 65335 seconds.

Command Default

Four times the interval set by the **ospfv3 h ello-interval** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 dead-interval**command to set the time period for which hello packets must not be seen before neighbors declare the router down. When the **ospfv3 dead-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 dead-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 dead-interval**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

If no hello-interval is specified, the default dead-interval is 120 seconds for Mobile Ad Hoc Networks (MANETs) and 40 seconds for all other network types.

Examples

The following example sets the OSPFv3 dead interval to 60 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 dead-interval 60
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 demand-circuit

To configure Open Shortest Path First version 3 (OSPFv3) to treat the interface as an OSPFv3 demand circuit, use the ospfv3 **demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ospfv3 [*process-id*] **demand-circuit** [**disable**] [**ignore**]
no ospfv3 demand-circuit

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Disables the demand circuit on the specified OSPFv3 instance.
ignore	(Optional) Ignores requests from other routers to operate the link in demand-circuit mode.

Command Default

The circuit is not a demand circuit.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was modified. The **ignore** keyword was added.

Usage Guidelines

Use the **ospfv3 demand-circuit**command to configure OSPFv3 to treat the interface as an OSPFv3 demand circuit. When the **ospfv3 demand-circuit**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf demand-circuit**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 demand-circuit**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

On point-to-point interfaces, only one end of the demand circuit must be configured with the **demand-circuit** command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example configures an on-demand circuit on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 demand-circuit
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 encryption

To specify the encryption type for an Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ospfv3 encryption {**ipsec spi** *spi* **esp** *encryption-algorithm key-encryption-type key authentication-algorithm key-encryption-type key* | **null**}
no ospfv3 encryption ipsec spi *spi*

Syntax Description

ipsec	Configures use of IP Security (IPsec) authentication.
spi *spi*	Security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295.
esp	Encapsulating security payload (ESP).
encryption-algorithm	Encryption algorithm to be used with ESP. The values can be any of the following: • **aes-cbc**--Enables AES-CBC encryption. • **3des**--Enables 3DES encryption. • **des**--Enables DES encryption. • **null**--ESP with no encryption.
key-encryption-type	One of two values can be entered: • **0** --The key is not encrypted. • **7** --The key is encrypted.
key	Number used in the calculation of the message digest. • When MD5 authentication is used, the key must be 32 hex digits (16 bytes) long. • When SHA-1 authentication is used, the key must be 40 hex digits (20 bytes) long.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5** --Enables message digest 5 (MD5). • **sha1** --Enables SHA-1.
null	Overrides area encryption.

Command Default

Authentication and encryption are not configured on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 encryption**command to specify the encryption type for an interface. The **ospfv3 encryption**command cannot be configured per process. If the **ospfv3 encryption**command is used, it affects all OSPFv3 instances.

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPFv3 and a tunnel, cannot use the same SPI. Additionally, an SPI can be used only in one policy.

The **null** keyword is used to override existing area encryption. If area encryption is not configured, then it is not necessary to configure the interface with the **encryption null**command.

Examples

The following example specifies the encryption type for Ethernet interface 0/0. The IPSec SPI value is 1001, ESP is used with no encryption, and the authentication algorithm is MD5.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ospfv3 encryption ipsec spi 1001 esp null md5 0
 27576134094768132473302031209727
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ospfv3 flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ospfv3 [*process-id*] **flood-reduction** [**disable**]
no ospfv3 [*process-id*] **flood-reduction**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
disable	(Optional) Allows flood reduction to be disabled on the specified OSPFv3 interface.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 flood-reduction**command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 flood-reduction**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf flood-reduction**configuration if OSPFv3 was attached to the interface using the ipv6 ospf flood-reduction command. When the **ospfv3 flood-reduction**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

All routers supporting the OSPFv3 demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example suppresses the flooding of unnecessary LSAs on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 flood-reduction
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the Open Shortest Path First version 3 (OSPFv3) interface, use the ospfv3 **hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ospfv3 [*process-id*] **hello-interval** *seconds*
no ospfv3 [*process-id*] **hello-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Command Default

The default interval is 10 seconds when using Ethernet and 30 seconds when using nonbroadcast, such as Mobile Ad Hoc Networks (MANETs).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 hello-interval**command to suppress unnecessary LSA flooding in stable topologies. When the **ospfv3 hello-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf hello-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 hello-interval**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

The **hello-interval** value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 hello-interval 15
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 mtu-ignore

To disable Open Shortest Path First version 3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ospfv3 mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ospfv3 [*process-id*] **mtu-ignore** [**disable**]
no ospfv3 [*process-id*] **mtu-ignore**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
disable	(Optional) Allows **mtu-ignore**to be disabled on the specified OSPFv3 interface.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 mtu-ignore**command to disable OSPFv3 MTU mismatch detection on receiving DBD packets. When the **ospfv3 mtu-ignore**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf mtu-ignore**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 mtu-ignore**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 mtu-ignore
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 network

To configure an Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for a given medium, use the ospfv3 **network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}
no ospfv3 [*process-id*] **network** {**broadcast** | **manet** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
broadcast	Sets the network type to broadcast.
manet	Sets the network type to Mobile Ad Hoc Network (MANET).
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint non-broadcast	Sets the network type to point-to-multipoint. The optional **non-broadcast** keyword sets the point-to-multipoint network to be nonbroadcast. If you use the **non-broadcast** keyword, the **neighbor** command is required.
point-to-point	Sets the network type to point-to-point.

Command Default

Default depends on the network type.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 network** command to configure an OSPFv3 network type to a type other than the default for a given medium. When the **ospfv3 network**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf network**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 network**command is configured without the *process-id* argument, it is inherited on all instances running on the interface. .

MANET Networks

Use the **ospfv3 network manet** command to enable relaying and caching of LSA updates and LSA ACKs on the MANET interface. This results in a reduction of OSPF traffic and saves radio bandwidth.

By default, selective peering is disabled on MANET interfaces.

By default, the OSPFv3 dynamic cost timer is enabled for the MANET network type, as well as caching of LSAs and LSA ACKs received on the MANET interface. The following default values are applied for cache and timers:

LSA cache	Default = 1000 messages
LSA timer	Default = 10 minutes
LSA ACK cache	Default = 1000 messages
LSA ACK timer	Default = 5 minutes

Examples

The following example sets your OSPFv3 network as a broadcast network:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 network broadcast
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 priority

To set the router priority, which helps determine the designated router for this network, use the ospfv3 **priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **priority** *number-value*
no ospfv3 [*process-id*] **priority** *number-value*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Command Default

The router priority is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 priority**command to set the router priority, which helps determine the designated router for this network. When the **ospfv3 priority**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf priority**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 priority**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Examples

The following example sets the router priority value to 4:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 priority 4
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **retransmit-interval** *seconds*
no ospfv3 [*process-id*] **retransmit-interval** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds, and the default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 retransmit-interval**command to specify the time between LSA retransmissions for adjacencies belonging to the interface. When the **ospfv3 retransmit-interval**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf retransmit-interval**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 retransmit-interval**command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of the restransmit-interval parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

ospfv3 transmit-delay

To set the estimated time required to send a link-state update packet on the Open Shortest Path First version 3 (OSPFv3) interface, use the **ospfv3 transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ospfv3 [*process-id*] **transmit-delay** *seconds*
no ospfv3 [*process-id*] **transmit-delay** *seconds*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Command Default

The default is 1 second.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ospfv3 transmit-delay**command to set the estimated time required to send a link-state update packet on the interface. When the **ospfv3 transmit-delay**command is configured with the *process-id* argument, it overwrites the **ipv6 ospf transmit-delay**configuration if OSPFv3 was attached to the interface using the ipv6 ospf area command. When the **ospfv3 transmit-delay** command is configured without the *process-id* argument, it is inherited on all instances running on the interface.

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
Router(config)# interface ethernet0/0
Router(config-if)# ospfv3 101 transmit-delay 3
```

Related Commands

Command	Description
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

other-config-flag

To verify the advertised “other” configuration parameter, use the **other-config-flag** command in RA guard policy configuration mode.

other-config-flag {**on** | **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

passive-interface (IPv6)

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [{**default** | *interface-type interface-number*}]
no passive-interface [{**default** | *interface-type interface-number*}]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

passive-interface (OSPFv3)

To suppress sending routing updates on an interface when using an IPv4 Open Shortest Path First version 3 (OSPFv3) process, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [{**default** | *interface-type interface-number*}]
no passive-interface [{**default** | *interface-type interface-number*}]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If you suppress the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0/0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

Related Commands

Command	Description
default (OSPFv3)	Returns an OSPFv3 parameter to its default value.

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

peer default ipv6 address pool

To specify the pool from which client prefixes are assigned, use the **peer default ipv6 address pool** command in interface configuration mode. To disable a prior peer IPv6 address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ipv6 address pool *pool-name*
no peer default ipv6 address pool

Syntax Description

pool-name	Name of a local address pool created using the **ipv6 local pool** command.

Command Default

The default pool name is **pool**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS 12.2(13)T	This command was introduced.

Usage Guidelines

Note Ensure that PPP authentication is enabled on the interface.

This command applies to point-to-point interfaces that support PPP encapsulation. This command sets the address used on the remote (PC) side.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.

Examples

The following command specifies that the interface will use a local IPv6 address pool named pool3:

```
peer default ipv6 address pool pool3
```

In the following example, the pool1 pool is assigned to virtual template 1:

```
interface Virtual-Template1
 encapsulation ppp
 ipv6 enable
 no ipv6 nd suppress-ra
 peer default ipv6 address pool pool1
 ppp authentication chap
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.

Command	Description
encapsulation ppp	Enables PPP encapsulation.
ipv6 local pool	Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface.
ppp	Starts an asynchronous connection using PPP.

permit (IPv6)

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

permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
no permit *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol
permit icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [{*icmp-type* [*icmp-code*]*icmp-message*}] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol
permit tcp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**neq** {*portprotocol*}] [**psh**] [**range** {*portprotocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol
permit udp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [{*doh-numberdoh-type*}]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [{*mh-numbermh-type*}]] [**neq** {*portprotocol*}] [**range** {*portprotocol*}] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, **udp**, or **hbh**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length	The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set permit conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with any protocol.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix/prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix/prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/ prefix-length	The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set permit conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dest-option-type	(Optional) Matches IPv6 packets against the destination extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.

fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified. When this keyword is used, it also matches when the first fragment does not have Layer 4 information.
hbh	(Optional) Matches IPv6 packets against the hop-by-hop extension header within each IPv6 packet header.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(mobility) Matches IPv6 packets against the mobility extension header within each IPv6 packet header.
mobility-type	(Optional) Matches IPv6 packets against the mobility-type extension header within each IPv6 packet header. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Mobility header types. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error

reflect *name*	(Optional) Specifies a reflexive IPvi6 access list. Reflexive IPv6 access lists are created dynamically when an IPv6 packets matches a permit statement that contains the **reflect** keyword. The reflexive IPv6 access list mirrors the permit statement and times out automatically when no IPv6 packets match the permit statement. Reflexive IPv6 access lists can be applied to the TCP, UDP, SCTP, and ICMP for IPv6 packets.
timeout *value*	(Optional) Interval of idle time (in seconds) after which a reflexive IPv6 access list times out. The acceptable range is from 1 to 4294967295. The default is 180 seconds.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Matches IPv6 packets against the routing-type extension header within each IPv6 packet header. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.

ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
{**range** *port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration (config-ipv6-acl)#

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.2(3)T	This command was modified. Support was added for the **hbh** keyword.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Release	Modification
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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

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

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

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

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

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

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

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

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

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable

- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Defining Reflexive Access Lists

To define an IPv6 reflexive list, a form of session filtering, use the **reflect** keyword in the **permit** (IPv6) command. The **reflect** keyword creates an IPv6 reflexive access list and triggers the creation of entries in the reflexive access list. The **reflect** keyword must be an entry (condition statement) in an IPv6 access list.

Note For IPv6 reflexive access lists to work, you must nest the reflexive access list using the **evaluate** command.

If you are configuring IPv6 reflexive access lists for an external interface, the IPv6 access list should be one that is applied to outbound traffic.

If you are configuring an IPv6 reflexive access list for an internal interface, the IPv6 access list should be one that is applied to inbound traffic.

IPv6 sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the IPv6 access list, the packet is also evaluated against the IPv6 reflexive permit entry.

As with all IPv6 access list entries, the order of entries is important, because they are evaluated in sequential order. When an IPv6 packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive permit entry, the packet will not be evaluated by the reflexive permit entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive permit entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive permit entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating that the packet belongs to a session in progress). The temporary entry specifies criteria that permit traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

The **permit** (IPv6) command with the **reflect** keyword enables the creation of temporary entries in the same IPv6 reflexive access list that was defined by the **permit** (IPv6) command. The temporary entries are created when an IPv6 packet exiting your network matches the protocol specified in the **permit** (IPv6) command. (The packet “triggers” the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a permit entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except that the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except that the port numbers are swapped.
- If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: The temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IPv6 traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IPv6 packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configured length of time (the timeout period), the entry will expire.

Examples

The following example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:ODB8:0300:0201::/64 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive access list named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network FEC0:0:0:0201::/64 (packets that have the site-local prefix FEC0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The third permit entry in the OUTBOUND list permits all ICMP packets to exit out of Ethernet interface 0.

The permit entry in the INBOUND list permits all ICMP packets to enter Ethernet interface 0. The **evaluate** command in the list applies the temporary IPv6 reflexive access list named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets. Refer to the **evaluate** command for more information on nesting IPv6 reflexive access lists within IPv6 ACLs.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any
ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT
interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

Note Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND access list, only TCP, UDP, and ICMP packets will be permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the access list denies all other packet types on the interface).

The following example shows how to allow the matching of any UDP traffic. The authentication header may be present.

```
permit udp any any sequence 10
```

The following example shows how to allow the matching of only TCP traffic if the authentication header is also present.

```
permit tcp any any auth sequence 20
```

The following example shows how to allow the matching of any IPv6 traffic where the authentication header is present.

```
permit ahp any any sequence 30
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
evaluate (IPv6)	Nests an IPv6 reflexive access list within an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

permit link-local

To allow hardware bridging for all data traffic sourced by a link-local address, use the **permit link-local** command in source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode. To disable this function, use the **no** form of this command.

permit link-local
no permit link-local

Syntax Description

This command has no arguments or keywords.

Command Default

This function is disabled.

Command Modes

Source-guard policy configuration (config-source-guard)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **permit link-local** command to allow hardware bridging for all data traffic sourced by a link-local address. This feature is used to reduce the number of ternary content addressable memory (TCAM) entries that are used. Because link-local addresses are valid only on the local link, they are not as critical to block as global addresses.

Use the **permit link-local** command after entering the **ipv6 source-guard policy** command to define an IPv6 source-guard policy name.

Examples

The following example shows how to allow hardware bridging for all data traffic sourced by a link-local address:

```
Device(config)# ipv6 source-guard policy mysgpolicy
Device(config-source-guard)# permit link-local
```

Related Commands

Command	Description
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

ping ipv6

To diagnose basic net work connectivity when using IPv6, use the **ping IPv6** command in user EXEC or privileged EXEC mode.

ping ipv6 *ipv6-address* [{**data** *hex-data-pattern* | **repeat** *repeat-count* | **size** *datagram-size* | **source** [{**async** | **bvi** | **ctunnel** | **dialer** | **ethernet** | **fastEthernet** | **gigabitEthernet** | **loopback** | **mfr** | **multilink** | **null** | **port-channel** | **tunnel** | **virtual-template***source-address* | **xtagatm**}] | **timeout** *seconds* | **verbose**}]

Syntax Description

ipv6-address	The address or hostname of the IPv6 host to be pinged. This address or hostname must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.
data	(Optional) Specifies the data pattern.
hex-data-pattern	(Optional) Range is from 0 to FFFF.
repeat	(Optional) Specifies the number of pings sent. The default is 5.
repeat-count	(Optional) Range is from 1 to 2147483647.
size	(Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping.
datagram-size	(Optional) Range is from 48 to 18024.
source	(Optional) Specifies the source address or name.
async	(Optional) Asynchronous interface.
bvi	(Optional) Bridge-Group Virtual Interface.
ctunnel	(Optional) CTunnel interface.
dialer	(Optional) Dialer interface.
ethernet	(Optional) Ethernet IEEE 802.3.
fastEthernet	(Optional) FastEthernet IEEE 802.3.
gigabitEthernet	(Optional) GigabitEthernet IEEE 802.3z.
loopback	(Optional) Loopback interface.
mfr	(Optional) Multilink frame relay (MFR) bundle interface.
multilink	(Optional) Multilink-group interface.
null	(Optional) Null interface.
port-channel	(Optional) Ethernet channel of interfaces.
tunnel	(Optional) Tunnel interface.

virtual-template	(Optional) Virtual template interface.
source-address	(Optional) Source IPv6 address or name.
xtagatm	(Optional) Extended Tag ATM interface.
timeout	(Optional) Specifies the timeout interval in seconds. The default is 2 seconds.
seconds	(Optional) Range is from 0 to 3600.
verbose	(Optional) Displays the verbose output.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The user-level ping feature provides a basic ping facility for users that do not have system privileges. This feature allows the Cisco IOS software to perform the simple default ping functionality for a number of protocols.

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

If the system cannot map an address for a hostname, it returns an "%Unrecognized host or address, or protocol not running" message.

To abnormally terminate a ping session, type the escape sequence--by default, Ctrl-^ X. You type the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

Caution When the **timeout** keyword is used with the *seconds* argument set to 0, an immediate timeout occurs, which causes a flood ping. Use the **timeout 0** parameter with caution, because you may receive replies only from immediately adjacent routers depending on router and network use, distance to the remote device, and other factors.

The table below describes the characters displayed by the ping facility in IPv6.

Table 9: ping Test Characters (IPv6)

!	Each exclamation point indicates receipt of a reply.
.	Each period indicates that the network server timed out while waiting for a reply.
?	Unknown error.
@	Unreachable for unknown reason.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
B	Packet too big.
C	Alignment errors.
H	Host unreachable.
N	Network unreachable (beyond scope).
P	Port unreachable.
R	Parameter problem.
S	Source address failed ingress/egress policy.
T	Time exceeded.
U	No route to host.
X	Reject route to destination.

Note Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are answered only by another Cisco router.

When the **ping ipv6** command is enabled, the router attempts to resolve hostnames into IPv6 addresses before trying to resolve them into IPv4 addresses, so if a hostname resolves to both an IPv6 and an IPv4 address and you specifically want to use the IPv4 address, use the **ping** (IPv4) command.

Examples

The following user EXEC example shows sample output for the **ping ipv6** command:

```
Router# ping ipv6 2001:0DB8::3/64
Target IPv6 address: 2001:0DB8::3/64
Repeat count [5]:
Datagram size [100]:48
Timeout in seconds [2]:
Extended commands? [no]: yes
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:yes
Include destination option? [no]:y
% Using size of 64 to accommodate extension headers
```

```
Sweep range of sizes? [no]:y
Sweep min size [100]: 100
Sweep max size [18024]: 150
Sweep interval [1]: 5
Sending 55, [100..150]-byte ICMP Echos to 2001:0DB8::3/64, timeout is 2 seconds:
Success rate is 100 percent
round-trip min/avg/max = 2/5/10 ms
```

The table below describes the default **ping ipv6** fields shown in the display.

Table 10: ping ipv6 Field Descriptions

Field	Description
Target IPv6 address:	Prompts for the IPv6 address or host name of the destination node you plan to ping. Default: none.
Repeat count [5]:	Number of ping packets that will be sent to the destination address. Default: 5.
Datagram size [100]:	Size of the ping packet (in bytes). Default: 100 bytes.
Timeout in seconds [2]:	Timeout interval (in seconds). Default: 2.
Extended commands [no]:	Specifies whether a series of additional commands appears. Default: no. In an IPv6 dialog for the **ping IPv6** command, entering yes in the Extended commands field displays the UDP protocol?, Verbose, Priority, and Include extension headers? fields.
UDP protocol? [no]:	Specifies UDP packets or ICMPv6 packets. Default: no (ICMP packets are sent).
Verbose? [no]:	Enables verbose output.
Precedence [0]:	Sets precedence in the IPv6 header. The range is from 0 to 7.
DSCP [0]:	Sets Dynamic Host Configuration Protocol (DSCP) in the IPv6 header. The range is from 0 to 63. DSCP appears only if the precedence option is not set, because precedence and DSCP are two separate ways of viewing the same bits in the header.
Include hop by hop option? [no]:	The IPv6 hop-by-hop option is included in the outgoing echo request header, requiring the ping packet to be examined by each node along the path and therefore not be fast-switched or Cisco Express Forwarding-switched. This function may help with debugging network connectivity, especially switching problems. **Note** A Cisco router also includes the hop-by-hop option in the returned echo reply, so the packets should be process-switched rather than fast-switched or Cisco Express Forwarding-switched on the return path also. Non-Cisco routers likely do not have this option in their echo reply; therefore, if the echo request with hop-by-hop option arrives at the destination but the echo reply does not come back and the destination is not a Cisco router, a fast-path issue may exist in an intermediate router.

Field	Description
Include destination option? [no]:	Includes an IPv6 destination option in the outgoing echo request header.
Sweep range of sizes? [no]:	Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced.
Sweep min size [100]: Sweep max size [18024]: Sweep interval [1]:	Options that appear if "Sweep range of sizes?" option is enabled. • Sweep min size--Defaults to the configured "Datagram size" parameter and will override that value if specified. • Sweep Interval--The size of the intervals between the "Sweep min size" and "Sweep max size" parameters. For example, min of 100 max of 150 with an interval of 5 means packets sent are of 100, 105, 110, ..., 150 bytes in size.
Sending 55, [100..150]-byte ICMP Echos to ...	Minimum and maximum sizes and interval as configured in "Sweep range of sizes" options. Sizes are reported if the ping fails (but not if it succeeds, unless the verbose option is enabled).
Success rate is 100 percent	Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic.
round-trip min/avg/max = 2/5/10 ms	Round-trip minimum, average, and maximum time intervals for the protocol echo packets (in milliseconds).

platform ipv6 acl fragment hardware

To permit or deny fragments at hardware, use the **platform ipv6 acl fragment hardware** command in global configuration mode. To reset the IPv6 fragment handling to bridged mode, use the **no** form of this command.

platform ipv6 acl fragment hardware {**forward** | **drop**}
no platform ipv6 acl fragment hardware {**forward** | **drop**}

Syntax Description

forward	Forwards the IPv6 fragments in the hardware.
drop	Drops the IPv6 fragments in the hardware.

Command Default

The **no** form of this command is the default behavior.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The PFC3A, PFC3B, and PFC3BXL are unable to handle IPv6 fragments in hardware, and all IPv6 fragments are handled in software. This could result in high CPU if your traffic includes a large amount of IPv6 fragments. This limitation is handled in the PFC3C hardware. The **platform ipv6 acl fragment hardware**command provides a software workaround for the PFC3A, PFC3B, and PFC3BXL by specifying either to permit or drop all IPv6 fragments in hardware.

Note When you enter the **drop** keyword, a small portion of the packets is leaked to the software (for ICMP message generation) and forwarded in software.

The **platform ipv6 acl fragment hardware** command overrides the following actions:

- Any ACE in the IPv6 filter (ACL) that contains the **fragment** keyword. If the ACE in the ACL contains the **fragment** keyword, the associated action (**permit** | **deny** | **log**) is not taken, and the action (**permit** | **drop**) specified by the **platform ipv6 acl fragment hardware** command is taken.
- Any IPv6 ACL that contains ACEs that implicitly permit IPv6 fragments; for example, permit ACEs that contain Layer 4 ports to implicitly permit fragments only.
- If the IPv6 fragment hits the implicit **deny any any** ACE added at the end of the ACL, the IPv6 fragment will not get hit.

Examples

This example shows how to forward the IPv6 fragments at hardware:

```
Router(config)#
platform ipv6 acl fragment hardware forward
```

This example shows how to drop the IPv6 fragments at hardware:

```
Router(config)#
platform ipv6 acl fragment hardware drop
```

platform ipv6 acl icmp optimize neighbor-discovery

To optimize ternary content addressable memory (TCAM) support for IPv6 access lists (ACLs), use the **platform ipv6 acl icmp optimize neighbor-discovery** command in global configuration mode. To disable optimization of TCAM support for IPv6 ACLs, use the **no** form of this command.

platform ipv6 acl icmp optimize neighbor-discovery
no platform ipv6 acl icmp optimize neighbor-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Use this command under the direction of the Cisco Technical Assistance Center only.

When you enable optimization of the TCAM support for IPv6 ACLs, the global Internet Control Message Protocol version 6 (ICMPv6) neighbor-discovery ACL at the top of the TCAM is programmed to permit all ICMPv6 neighbor-discovery packets. Enabling optimization prevents the addition of ICMPv6 access control entries (ACEs) at the end of every IPv6 security ACL, reducing the number of TCAM resources being used. Enabling this command reprograms IPv6 ACLs on all interfaces.

Note The ICMPv6 neighbor-discovery ACL at the top of the TCAM takes precedence over security ACLs for ICMP neighbor-discovery packets that you have configured, but has no effect if you have a bridge/deny that overlaps with the global ICMP ACL.

Examples

This example shows how to optimize TCAM support for IPv6 ACLs:

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery
```

This example shows how to disable optimization of TCAM support for IPv6 ACLs:

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery
```

platform ipv6 acl punt extension-header

To enable processing of IPv6 packets with extension headers in software on the RP, use the **platform ipv6 acl punt extension-header**command in global configuration mode. To disable processing of IPv6 packets with extension headers in software on the RP, use the **no** form of this command.

platform ipv6 acl punt extension-header
no platform ipv6 acl punt extension-header

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 packets with extension headers are processed in software.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(33)SXH7	This command was introduced on the Supervisor Engine 720.
15.2(2)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

If your IPv6 traffic does not specify a Layer 4 protocol, software processing of IPv6 packets with extension headers is unnecessary. If your IPv6 traffic specifies a Layer 4 protocol, you can enter the **platform ipv6 acl punt extension-header** global configuration command to enable software processing of IPv6 packets with extension headers. On the Cisco 7600 series routers, this command is applicable only on the line cards that use Pinnacle as the port ASIC. Examples for such line cards include WS-X6548-GE-TX, WS-X6516A-GBIC, WS-X6516-GBIC, WS-X6148-GE-TX, and WS-X6816-GBIC.

Examples

This example shows how to enable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# platform ipv6 acl punt extension-header
Router(config)#
```

This example shows how to disable processing of IPv6 packets with extension headers in software on the RP:

```
Router(config)# no platform ipv6 acl punt extension-header
Router(config)#
```

poison-reverse (IPv6 RIP)

To configure the poison reverse processing of IPv6 Routing Information Protocol (RIP) router updates, use the **poison-reverse**command in router configuration mode. To disable the poison reverse processing of IPv6 RIP updates, use the **no** form of this command.

poison-reverse
no poison-reverse

Syntax Description

This command has no keywords or arguments

Command Default

Poison reverse is not configured.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command configures poison reverse processing of IPv6 RIP router updates. When poison reverse is configured, routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric.

If both poison reverse and split horizon are configured, then simple split horizon behavior (suppression of routes out of the interface over which they were learned) is replaced by poison reverse behavior.

Examples

The following example configures poison reverse processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# poison-reverse
```

Related Commands

Command	Description
split-horizon (IPv6 RIP)	Configures split horizon processing of IPv6 RIP router updates.

port (IPv6 RIP)

To configure a specified UDP port and multicast address for an IPv6 Routing Information Protocol (RIP) routing process, use the **port** command in RIP router configuration mode. To return the port number and multicast address to their default values, use the **no** form of this command.

port *port-number* **multicast-group** *multicast-address*
no port *port-number* **multicast-group** *multicast-address*

Syntax Description

port-number	UDP port number. The range is from 1 to 65535. The table in the "Usage Guidelines" section lists common UDP services and their port numbers.
multicast-group	Specifies a multicast group.
multicast-address	Address or hostname of the multicast group.

Command Default

UDP port 521; multicast address FF02::9

Command Modes

RIP router configuration (config-rtr-rip)

Command History

Release	Modification
Cisco IOS 12.2(2)T	This command was introduced.
Cisco IOS 12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
Cisco IOS 12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
Cisco IOS 12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
Cisco IOS 12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS 12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS 12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS 12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS 15.4(1)S	This command was deprecated.
Cisco IOS 15.4(1)T	This command was deprecated.

Usage Guidelines

Two IPv6 RIP routing processes cannot use the same UDP port. If two IPv6 RIP routing processes are configured on the same UDP port, the second process will not start until the configuration conflict is resolved. Two IPv6 RIP routing processes, though, can use the same multicast address. UDP services and port numbers are shown in the table below.

Table 11: Common UDP Services and Their Port Numbers

Service	Port
Domain Name System (DNS)	53
Network File System (NFS)	2049
remote-procedure call (RPC)	111
Simple Network Management Protocol (SNMP)	161
Trivial File Transfer Protocol (TFTP)	69

Examples

The following example configures UDP port 200 and multicast address FF02::9 for the IPv6 RIP routing process named cisco:

```
Device(config)# ipv6 router rip cisco
Device(config-rtr-rip)# port 200 multicast-group FF02::9
```

port (TACACS+)

To specify the TCP port to be used for TACACS+ connections, use the **port**command in TACACS+ server configuration mode. To remove the TCP port, use the **no** form of this command.

port [*number*]
no port [*number*]

Syntax Description

number	(Optional) Specifies the port where the TACACS+ server receives access-request packets. The range is from 1 to 65535.

Command Default

If no port is configured, port 49 is used.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

TCP port 49 is used if the *number* argument is not used when using the **port** command.

Examples

The following example shows how to specify TCP port 12:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

ppp ipv6cp address unique

To verify if the IPv6 prefix delegation is unique using a PP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated, use the **ppp ipv6cp address unique**command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ppp ipv6cp address unique
no ppp ipv6cp address unique

Syntax Description

This command has no arguments or keywords.

Command Default

Verification of the uniqueness of the IPv6 prefix delegation is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to verify whether the IPv6 prefix delegation is unique using a PPP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated:

```
Router> enable

Router# configure terminal
Router(config)# interface virtual-template 5
Router(config-if)# ppp ipv6cp address unique
```

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [**bap**]
no ppp multilink [**bap** [**required**]]

Cisco 10000 Series Router
ppp multilink
no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Command Default

This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(31)SB 2	This command was integrated into Cisco IOS Release 12.2(31)SB 2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink**command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the MLP bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Cisco 10000 Series Router

The ppp multilink command has no arguments or keywords.

Examples

The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.

Command	Description
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp ncp override local

To track attributes received in authorization from RADIUS, verify the permitted Network Control Program (NCP), reject the current NCP negotiation, and override the local dual-stack configuration, use the **ppp ncp override local**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ppp ncp override local
no ppp ncp override local

Syntax Description

This command has no arguments or keywords.

Command Default

The tracking of attributes from RADIUS and the local configuration override are not enabled. The local configuration is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Framed attributes are primarily used for address allocation. The RADIUS server maintains a pool of both IPv4 addresses and IPv6 prefixes. If IPv4 address or IPv6 prefix attributes are absent in the access-accept response from RADIUS, the **ppp ncp override local** command can be used to override local configuration.

Examples

The following example shows how to override the local IPv6 or IPv4 dual-stack configuration:

```
Router> enable

Router# configure terminal
Router(config)# ppp ncp override local
```

prc-interval (IPv6)

To configure the hold-down period between partial route calculations (PRCs), use the **p rc-interval**command in address family configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds* [*initial-wait*] [*secondary-wait*]
no **prc-interval** *seconds*

Syntax Description

seconds	Minimum amount of time between PRCs, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first PRC in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second PRC in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **prc-interval**command is used only in multitopology Intermediate System-to-Intermediate System (IS-IS).

The **prc-interval**command controls how often Cisco IOS software can perform a PRC. Increasing the PRC interval reduces the processor load of the router, but it could slow the convergence.

This command is analogous to the **spf-interval** command, which controls the hold-down period between shortest path first (SPF) calculations.

You can use the **prc-interval** (IPv6) command only when using the IS-IS multitopology for IPv6 feature.

Examples

The following example sets the PRC calculation interval to 20 seconds:

```
Router(config)# router isis
```

```
Router(config-router)# address-family ipv6
Router(config-router-af)# prc-interval 20
```

Related Commands

Command	Description
spf-interval (IPv6)	Controls how often Cisco IOS software performs the SPF calculation.

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [*lifetime*]
no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.
lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • **valid-lifetime** --The length of time, in seconds, that the prefix remains valid for the requesting router to use. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • **preferred-lifetime** --The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45** • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

Command Default

No manually configured prefix delegations exist.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation***prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the iaid in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-delegation aaa

To specify that prefixes are to be acquired from authorization, authentication, and accounting (AAA) servers, use the **prefix-delegation aaa**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

Cisco IOS Release 12.4(22)T and Earlier Releases and Cisco IOS Release 12.2(18)SXE, Cisco IOS XE Release 2.1, and Later Releases

prefix-delegation aaa [**method-list** *method-list* [**lifetime**] {{*valid-lifetime* | **infinite**} {*valid-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Cisco IOS Release 15.0(1)M and Later Releases

prefix-delegation aaa method-list {*method-list* | **default**} [{**lifetime** {*valid-lifetime* | **infinite**} {*preferred-lifetime* | **infinite**} | **at** {*date month year time* | *month date year time*} {*date month year time* | *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Syntax Description

method-list	(Optional) Indicates a method list to be defined.
method-list	Configuration type AAA authorization method list that defines how authorization will be performed.
default	Specifies the default method list, nvgened.
lifetime	(Optional) Configures prefix lifetimes.
valid-lifetime	The length of time that the prefix remains valid for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 2592000 seconds.
infinite	Indicates an unlimited lifetime.
preferred-lifetime	The length of time that the prefix remains preferred for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 604800 seconds.
at	Specifies absolute points in time where the prefix is no longer valid and no longer preferred.
date	The date for the valid lifetime to expire.
month	The month for the valid lifetime to expire.
year	The year for the valid lifetime to expire. The range is from 2003 to 2035.
time	The year for the valid lifetime to expire.

Command Default

The default time that the prefix remains valid is 2592000 seconds, and the default time that the prefix remains preferred for the requesting router to use is 604800 seconds.

Command Modes

DHCP for IPv6 pool configuration (config-dhcpv6)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **default** keyword was added and the command syntax was modified to show that **lifetime** can be configured only to a **method-list**.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, you must also configure the AAA client and Point-to-Point Protocol (PPP) on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

Use the **aaa authorization configuration default**, **aaa group server radius**, and **radius-server host** commands to specify a named list of authorization method and RADIUS servers to contact to acquire prefixes, and then apply that named list to the **prefix-delegation aaa** command.

Valid and preferred lifetimes can be specified for the prefixes assigned from AAA servers.

The **prefix-delegation aaa** and **prefix-delegation pool** commands are mutually exclusive in a pool.

Examples

The following example shows how to specify the use of a method list named list1:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp pool name
Router(config-dhcpv6)# prefix-delegation aaa method-list list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
radius-server host	Specifies a RADIUS server host.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server’s IPv6 address list option to clients.

Command	Description
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool**command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime** *valid-lifetime* *preferred-lifetime*]
no prefix-delegation pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
lifetime	(Optional) Used to set a length of time for the hosts to remember router advertisements. If the optional **lifetime** keyword is configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time that the prefix remains valid for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.
preferred-lifetime	The length of time, in seconds, that the prefix remains preferred for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**

Command Default

No IPv6 local prefix pool is specified. Valid lifetime is 2592000 seconds (30 days). Preferred lifetime is 604800 seconds (7 days).

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **prefix-delegation pool**command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation	Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-glean

To enable the device to glean prefixes from IPv6 router advertisements (RAs) or Dynamic Host Configuration Protocol (DHCP), use the **prefix-glean** command in IPv6 snooping configuration mode. To learn only prefixes gleaned in one of these protocols and exclude the other, use the **no** form of this command.

prefix-glean [**only**]
no prefix-glean [**only**]

Syntax Description

only	(Optional) Only prefixes are gleaned. Host addresses are not gleaned.

Command Default

Prefixes are not learned through RA or DHCP.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **prefix-glean** command enables the device to learn prefixes in RA and DHCP traffic.

Examples

The following example shows how to enable the device to learn prefixes:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# prefix-glean
```

Related Commands

Command	Description
ipv6 snooping attach-policy	Applies an IPv6 snooping policy to a target.
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

protocol (IPv6)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP) or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

protocol {**dhcp** | **ndp**} [{**prefix-list** *prefix-list-name*}]
no protocol {**dhcp** | **ndp**}

Syntax Description

dhcp	Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
ndp	Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.
prefix-list *prefix-list-name*	(Optional) Specifies that a prefix list of protected prefixes be used.

Command Default

Snooping and recovery are attempted using both DHCP and NDP. No prefix list is used, all address ranges are accepted.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- If a prefix list is specified, the prefix list applies to all flows for the specified protocol.
- If there is no prefix list specified, all protocols are supported by default. There is no check and all addresses are accepted.
- Using the **no protocol** {**dhcp** | **ndp**} command indicates that a protocol will not to be used for snooping or gleaning.
- However, if the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- The NDP prefix list should be a superset of the DHCP prefix list, as addresses obtained by DHCP must be confirmed by NDP later.
- When a prefix list is given and a protocol packet indicates an address that does not match the prefix list for that protocol, the packet is dropped (unless the security level is “glean”).

  This means that if the security level is "glean" all packets are gleaned - without checking the prefix-list. If the security level is "guard", then packets are checked againt the policy-configured prefix-list, to allow or deny it.

- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

Note Before you configure the **protocol** command, it is essential that you provide a value for the **ge** *ge-value* option when configuring a prefix list using the **ipv6 prefix-list** command.

Examples

The following example shows a valid configuration for an IPv6 prefix list ("abc") and shows that DHCP will be used to recover addresses that match the prefix list abc:

```
Device(config)# ipv6 prefix-list abc seq 5 permit 2001:DB8::/64 ge 128
!
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 snooping policy	Enters IPv6 snooping configuration mode.

protocol ipv6 (ATM)

To map the IPv6 address of a remote node to the ATM permanent virtual circuit (PVC) used to reach the address, use the **protocol ipv6**command in ATM VC configuration mode. To remove the static map, use the **no** form of this command.

protocol ipv6 *ipv6-address* [[**no**] **broadcast**]
no protocol ipv6 *ipv6-address* [[**no**] **broadcast**]

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a PVC . This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no broadcast	(Optional) Indicates whether the map entry should be used when IPv6 multicast packets (not broadcast packets) are sent to the interface. Pseudobroadcasting is supported. The [**no**] **broadcast** keywords in the **protocol ipv6** command take precedence over the **broadcast** command configured on the same ATM PVC.

Command Default

No mapping is defined.

Command Modes

ATM VC configuration (for an ATM PVC)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

In the following example, two nodes named Cisco 1 and Cisco 2 are connected by a single PVC. The point-to-point subinterface ATM0.132 is used on both nodes to terminate the PVC; therefore, the mapping between the IPv6 addresses of both nodes and the PVC is implicit (no additional mappings are required).

Cisco 1 Configuration

```
interface ATM0
```

```
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

In the following example, the same two nodes (Cisco 1 and Cisco 2) from the previous example are connected by the same PVC. In this example, however, the point-to-multipoint interface ATM0 is used on both nodes to terminate the PVC; therefore, explicit mappings are required between the link-local and global IPv6 addresses of interface ATM0 on both nodes and the PVC. Additionally, ATM pseudobroadcasts are enabled on the link-local address of interface ATM0 on both nodes.

Cisco 1 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 2001:0DB8:2222::45
  protocol ipv6 FE80::60:2FA4:8291:2 broadcast
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```
interface ATM0
 no ip address
 pvc 1/32
  protocol ipv6 FE80::60:3E47:AC8:C broadcast
  protocol ipv6 2001:0DB8:2222::72
  encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222::45/32
```

Related Commands

Command	Description
show atm map	Displays the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps.

queue-depth (OSPFv3)

To configure the number of incoming packets that the IPv4 Open Shortest Path First version 3 (OSPFv3) process can keep in its queue, use the **queue-depth** command in OSPFv3 router configuration mode. To set the queue depth to its default value, use the **no** form of the command.

queue-depth {**hello** | **update**} {*queue-size* | **unlimited**}
no queue-depth {**hello** | **update**}

Syntax Description

hello	Specifies the queue depth of the OSPFv3 hello process.
update	Specifies the queue depth of the OSPFv3 router process queue.
queue-size	Maximum number of packets in the queue. The range is 1 to 2147483647.
unlimited	Specifies an infinite queue depth.

Command Default

If you do not set a queue size, the OSPFv3 hello process queue depth is unlimited and the OSPFv3 router process (update) queue depth is 200 packets.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

All incoming OSPFv3 packets are initially enqueued in the hello queue. OSPFv3 hello packets are processed directly from this queue, while all other OSPFv3 packet types are subsequently enqueued in the update queue.

If you configure a router with many neighbors and a large database, use the **queue-depth** command to adjust the size of the hello and router queues. Otherwise, packets might be dropped because of queue limits, and OSPFv3 adjacencies may be lost.

Examples

The following example shows how to configure the OSPFv3 update queue to 1500 packets:

```
Router(config)# router ospfv3 1
Router(config-router)# queue-depth update 1500
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute source-protocol [*process-id*] [**include-connected** {**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**tag** *tag-value*] [**route-map** *map-tag*]
no redistribute source-protocol [*process-id*] [**include-connected**] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [{**1** | **2**}] | **internal** | **nssa-external** [{**1** | **2**}]}] [**tag** *tag-value*] [**route-map** *map-tag*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, connected, **eigrp**, **isis**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp**keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis**keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, the process ID is the number assigned administratively when the Open Shortest Path First (OSPF) for IPv6 routing process is enabled. For the **rip**keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
include-connected	(Optional) Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
level-1	Specifies that, for Intermediate System-to-Intermediate System (IS-IS), Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
as-number	(Optional) Autonomous system number for the redistributed route.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

metric-type *type-value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If no value is specified for the **metric-type** keyword, the Cisco IOS software adopts a Type 2 external route. For IS-IS, the link type can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. • **rib-metric-as-external**—Sets metric type to external and uses the RIB metric. • **rib-metric-as-internal**—Sets metric type to internal and uses the RIB metric. The default is **internal**.
match {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]	(Optional) For OSPF, routes are redistributed into other routing domains using the match keyword. It is used with one of the following: • **external** [**1** | **2**] —Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • **internal** —Routes that are internal to a specific autonomous system. • **nssa-external** [**1**| **2**]—Routes that are external to the autonomous system but are imported into OSPF, in a not so stubby area (NSSA), for IPv6 as Type 1 or Type 2 external routes.
tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from BGP and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be checked to filter the importation of routes from this source routing protocol to the current routing protocol. If the route-map keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.

Command Default

Route redistribution is disabled.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.15S	This command was modified. The **rib-metric-as-external** and **rib-metric-as-internal** keywords were added.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **include-connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** router configuration command. Use of the **distribute-list prefix-list** command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6 this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the include-connected keyword. In IPv6 this functionality is not supported when the source protocol is BGP.

When the **no redistribute** command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the redistribute command only.

The default redistribute type will be restored to OSPF when all route type values are removed by the user.

Examples

The following example configures IPv6 IS-IS to redistribute IPv6 BGP routes. The metric is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

The following example redistributes IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# redistribute bgp 42
```

The following example redistributes IS-IS for IPv6 routes into the OSPF for IPv6 routing process 1:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

In the following example, ospf 1 redistributes the prefixes 2001:1:1::/64 and 2001:99:1::/64 and any prefixes learned through rip 1:

```
interface ethernet0/0
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable
interface ethernet1/1
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable
interface ethernet2/0
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1
ipv6 router ospf 1
  redistribute rip 1 include-connected
```

The following configuration example and output show the no redistribute command parameters when the last route type value is removed:

```
Router(config-router)# redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1 metric 7
Router(config-router)# no redistribute rip process1 metric 7
```

```
Router(config-router)# do show run | include redistribute
 redistribute rip process1
Router(config-router)#
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
distribute-list prefix-list (IPv6 EIGRP)	Applies a prefix list to EIGRP for IPv6 routing updates that are received or sent on an interface.
distribute-list prefix-list (IPv6 RIP)	Applies a prefix list to IPv6 RIP routing updates that are received or sent on an interface.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.

redistribute (OSPFv3)

To redistribute IPv6 and IPv4 routes from one routing domain into another routing domain, use the **redistribute** command in IPv6 or IPv4 address family configuration mode. To disable redistribution, use the **no** form of this command.

redistribute **source-protocol** [*process-id*] [*options*]
no **redistribute** **source-protocol** [*process-id*] [*options*]

Syntax Description

source-protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, connected, **eigrp**, **isis**, **nd**, **nemo**, **ospfv3**, **ospf**, **rip**, or **static**.
process-id	(Optional) For the **bgp** or **eigrp** keyword, the process ID is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospfv3** keyword, the process ID is the number assigned administratively when the Open Shortest Path First version 3 (OSPFv3) routing process is enabled. For the **rip** keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.
options	(Optional) The range of available options depends on the protocol. In OSPFv3, it includes the **nssa-only** keyword, which you can use to restrict external distributions to the not-so-stubby area (NSSA).

Command Default

Default redistribute type is OSPFv3.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was modified. The **nssa-only** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

For the IPv6 address family (AF), the **ospf** option refers to an OSPFv3 process. For the IPv4 address family, the **ospfv3** option specifies an OSPFv3 process, and the **ospf** option refers to an OSPFv2 process.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the include-connected keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute**command to advertise static routes as if they were directly connected routes.

Caution Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list**router configuration command. Use of the **distribute-list prefix-list**command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Note The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Note In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6, this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the include-connected keyword. In IPv6, this functionality is not supported when the source protocol is BGP.

When the no redistribute command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution will be removed completely when IS-IS level 1 and level 2 are removed by the user. IS-IS level settings can be configured using the redistribute command only.

The default redistribute type will be restored to OSPFv3 when all route type values are removed by the user.

Specify the **nssa-only** keyword to clear the propagate bit (P-bit) when external routes are redistributed into a NSSA. Doing so prevents corresponding NSSA external link state advertisements (LSAs) being translated into other areas.

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

redistribute isis (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain using Intermediate System-to-Intermediate System (IS-IS) as both the target and source protocol, use the **redistribute isis** command in address family configuration mode. To disable redistribution, use the **no** form of this command.

redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} {**distribute-list** *list-name* | **route-map** *map-tag*}
no redistribute isis [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} {**distribute-list** *list-name* | **route-map***map-tag*}

Syntax Description

process-id	(Optional) A *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.
level-1	Specifies that IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-2	Specifies that IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
into	Distributes IS-IS Level 1 or Level 2 routes into Level 1 or Level 2 in another IS-IS instance.
distribute-list	Specifies the distribute list used for the redistributed route.
list-name	Specifies the name of the distribute list for the redistributed route.
route-map *map-tag*	(Optional) Specifies the name of a route map that controls the IS-IS redistribution. You can specify either a distribute list or a route map, but not both.

Command Default

Route redistribution is disabled. No process ID is defined.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Aggregation Services Routers.
Cisco IOS XE Release 3.6S	This command was modified. Support for the **route-map** keyword was introduced.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the connected keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Examples

The following example shows how to redistribute only Level-1 routes with tag 100 to Level 2:

```
router isis
address-family ipv6
redistribute isis level-1 into level-2 route-map match-tag
route-map match-tag
match tag 100
```

Related Commands

Command	Description
default-metric	Specifies a default metric for redistributed routes.
ipv6 route priority high	Assigns a high priority to an IS-IS IPv6 prefix.
isis ipv6 tag	Configures an administrative tag value that will be associated with an IPv6 address prefix and applied to an IS-IS LSP.
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style type, length, and value.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.
show isis database verbose	Displays details about the IS-IS link-state database, including the route tag.
summary-prefix (IPv6 IS-IS)	Creates aggregate IPv6 prefixes for IS-IS.

register (mobile router)

To con trol the registration parameters of the IPv6 mobile router, use the **register** command in mobile router configuration mode or IPv6 mobile router configuration mode. To return the registration parameters to their default settings, use the **no** form of this command.

register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial milliseconds maximum milliseconds retry number**}
no register {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial milliseconds maximum milliseconds retry number**}

Syntax Description

extend	Reregisters before the lifetime expires.
expire *seconds*	Specifies the time (in seconds) in which to send a registration request before expiration. In IPv4, the range is from 1 to 3600; the default is 120. In IPv6, the range is from 1 to 600.
retry *number*	Specifies the number of times the mobile router retries sending a registration request if no reply is received. In both IPv4 and IPv6, the range is from 0 to 10; the default is 3. A value of 0 means no retry. The mobile router stops sending registration requests after the maximum number of retries is attempted.
interval *seconds*	Specifies the time (in seconds) that the mobile router waits before sending another registration request if no reply is received. In IPv4, the range is from 1 to 3600; the default is 10. In IPv6, the range is from 1 to 60.
lifetime *seconds*	Specifies the requested lifetime (in seconds) of each registration. The shortest value between the configured lifetime and the foreign agent advertised registration lifetime is used. In IPv4, the range is from 3 to 65534; the default is 65534 (infinity). In IPv6, the range is from 4 to 262143; the default is 262143 (infinity). This default ensures that the advertised lifetime is used, excluding infinity.
retransmit initial *milliseconds*	Specifies the wait period (in milliseconds) before sending a retransmission the first time no reply is received from the foreign agent. In IPv4, the range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second). In IPv6, the range is from 1000 to 256000.
maximum *milliseconds* **retry** *number*	Specifies the maximum wait period (in milliseconds) before retransmission of a registration request. In IPv4, the range is 10 to 10000 (10 seconds); the default is 5000 milliseconds (5 seconds). In IPv6, the maximum range is from 1000 to 256000. In IPv6, the retry number range is from 0 to 10. Each successive retransmission timeout period is twice the previous period, if the previous period was less than the maximum value. Retransmission stops after the maximum number of retries.

Command Default

The registration parameters of the IPv6 mobile router are used.

Command Modes

Mobile router configuration
IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The **register lifetime***seconds*command configures the lifetime that the mobile router requests in a registration request. The home agent also has lifetimes that are set. If the registration request from a mobile router has a greater lifetime than the registration reply from the home agent, the lifetime set on the home agent will be used for the registration. If the registration request lifetime from the mobile router is less than the registration reply from the home agent, the lifetime set on the mobile router will be used. Thus, the smaller lifetime between the home agent and mobile router is used for registration.

Examples

The following example specifies a registration lifetime of 600 seconds:

```
ip mobile router
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.

remark (IPv6)

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

remark *text-string*
no remark *text-string*

Syntax Description

text-string	Comment that describes the access list entry, up to 100 characters long.

Command Default

IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

The remark can be up to 100 characters long; anything longer is truncated.

Examples

The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet.

```
ipv6 access-list TELNETTING
 remark Do not allow Marketing subnet to telnet out
 deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

Related Commands

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

IPv6 Commands: ro to show bgp la

router ospfv3

To enter Open Shortest Path First version 3 (OSPFv3) router configuration mode, use the router ospfv3 command in interface configuration mode.

router ospfv3 [*process-id*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.

Command Default

No OSPFv3 routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **router ospfv3** command to enter the OSPFv3 router configuration mode. From this mode, you can enter address-family configuration mode for IPv6 or IPv4 and then configure the IPv6 or IPv4 AF.

Examples

The following example enters OSPFv3 router configuration mode:

```
Router(config)# router ospfv3 1
Router(config-router)#
```

Related Commands

Command	Description
ipv6 ospf area	Enables OSPFv3 on an interface
ospfv3 area	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF.

router-id (IPv6)

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) for IPv6 to use the previous OSPF for IPv6 router ID behavior, use the **no** form of this command.

router-id *router-id*
no router-id *router-id*

Syntax Description

router-id	Router ID for this OSPF process.

Command Default

The router ID is chosen automatically.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

OSPF for IPv6 (or OSPF version 3, or OSPFv3) is backward-compatible with OSPF version 2. In OSPFv3 and OSPF version 2, the router uses the 32-bit IPv4 address to select the router ID for an OSPF process. If an IPv4 address exists when OSPFv3 is enabled on an interface, then that IPv4 address is used for the router ID. If more than one IPv4 address is available, a router ID is chosen using the same rules as for OSPF version 2. If no IPv4 addresses are configured, the router selects a router ID automatically. Each router ID must be unique.

If this command is used on an OSPF for IPv6 router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPFv3 process restart. To manually restart the OSPFv3 process, use the **clear ipv6 ospf process**command.

Examples

The following example specifies a fixed router ID:

```
Router(config-rtr)# router-id 10.1.1.1
```

Related Commands

Command	Description
clear ipv6 ospf	Clears the OSPF for IPv6 state based on the OSPF routing process ID.

Command	Description
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.

router-id (OSPFv3)

To use a fixed router ID, use the **router-id** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To force OSPFv3 to use the previous OSPFv3 router ID behavior in IPv4, use the **no** form of this command.

router-id *router-id*
no router-id *router-id*

Syntax Description

router-id	Router ID for this OSPFv3 process.

Command Default

The router ID is chosen automatically.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

OSPFv3 is backward-compatible with OSPF version 2. In OSPFv3 and OSPF version 2, the router uses the 32-bit IPv4 address to select the router ID for an OSPFv3 process. If an IPv4 address exists when OSPFv3 is enabled on an interface, then that IPv4 address is used for the router ID. If more than one IPv4 address is available, a router ID is chosen using the same rules as for OSPF version 2. If no IPv4 addresses are configured, the router selects a router ID automatically. Each router ID must be unique.

If this command is used on an OSPFv3 router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPFv3 process restart.

Examples

The following example specifies a fixed router ID:

```
Router(config-router)# router-id 10.1.1.1
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in RA guard policy configuration mode.

router-preference maximum {**high** | **low** | **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default routers advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised default router preference is set to **high** in the received packet, then the packet is dropped. If the command option is set to **medium** or **low** in the received packet, then the packet is not dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures router-preference maximum verification to be high:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# router-preference maximum high
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*
no sec-level minimum *value*

Syntax Description

value	Minimum security level, which is a value from 1 to 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and specifies 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name**command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*
no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

Command	Description
aaa group server tacacs	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

set ipv6 default next-hop

To specify an IPv6 default next hop to which matching packets are forwarded, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete the default next hop, use the **no** form of this command.

set ipv6 default [{**vrf** *vrf-name* | **global**}] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]
no set ipv6 default [{**vrf** *vrf-name* | **global**}] **next-hop** *global-ipv6-address* [*global-ipv6-address...*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies explicitly that the default next-hops are under the specific Virtual Routing and Forwarding (VRF) instance.
global	(Optional) Specifies explicitly that the default next-hops are under the global routing table.
global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Packets are not forwarded to a default next hop.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument.

Use the **set ipv6 default next-hop** command in policy-based routing PBR for IPv6 to specify an IPv6 next-hop address to which a packet is policy routed when the router has no route in the IPv6 routing table or the packets match the default route. The IPv6 next-hop address must be adjacent to the router; that is, reachable by using a directly connected IPv6 route in the IPv6 routing table. The IPv6 next-hop address also must be a global IPv6 address. An IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

If the software has no explicit route for the destination in the packet, then the software routes the packet to the next hop as specified by the **set ipv6 default next-hop** command. The optional specified IPv6 addresses are tried in turn.

Use the **ipv6 policy route-map** command, the **route-map** command, and the **match** and **set route-map** commands to define the conditions for PBR packets. The **ipv6 policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which PBR occurs. The **set** commands specify the set actions, which are the particular routing actions to perform if the criteria enforced by the match commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Note The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands. The **set ipv6 next-hop** command is used to policy route packets for which the router has a route in the IPv6 routing table. The **set ipv6 default next-hop** command is used to policy route packets for which the router does not have a route in the IPv6 routing table (or the packets match the default route).

Examples

The following example shows how to set the next hop to which the packet is routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8:4:1::1/64 any
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 default next-hop 2001:DB8:4:4::1/64
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 policy-based routing (PBR) on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.

Command	Description
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 next-hop (BGP)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}
no set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}

Syntax Description

ipv6-address	IPv6 global address of the next hop to which packets are output. It need not be an adjacent router. 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-address	(Optional) IPv6 link-local address of the next hop to which packets are output. It must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	Name of the Layer 3 encapsulation profile.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default

IPv6 packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate l3vpn** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

The **set** commands specify the *set actions* --the particular routing actions to perform if the criteria enforced by the **match** commands are met.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ipv6 next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Configuring the **set ipv6 next-hop** *ipv6-address* command on a VRF interface allows the next hop to be looked up in a specified VRF address family. In this context, the *ipv6-address* argument matches that of the specified VRF instance.

Examples

The following example configures the IPv6 multiprotocol BGP peer FE80::250:BFF:FE0E:A471 and sets the route map named nh6 to include the IPv6 next hop global addresses of Fast Ethernet interface 0 of the neighbor in BGP updates. The IPv6 next hop link-local address can be sent to the neighbor by the nh6 route map or from the interface specified by the **neighbor update-source** router configuration command.

```
router bgp 170
 neighbor FE80::250:BFF:FE0E:A471 remote-as 150
 neighbor FE80::250:BFF:FE0E:A471 update-source fastether 0
address-family ipv6
  neighbor FE80::250:BFF:FE0E:A471 activate
  neighbor FE80::250:BFF:FE0E:A471 route-map nh6 out
route-map nh6
 set ipv6 next-hop 3FFE:506::1
```

Note If you specify only the global IPv6 next hop address (the *ipv6-address* argument) with the **set ipv6 next-hop** command after specifying the neighbor interface (the *interface-type* argument) with the **neighbor update-source** command, the link-local address of the neighbor interface is included as the next hop in the BGP updates. Therefore, only one route map that sets the global IPv6 next hop address in BGP updates is required for multiple BGP peers that use link-local addresses.

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.

Command	Description
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
neighbor next-hop-self	Disables next-hop processing of BGP updates on the router.
neighbor update-source	Specifies that the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ipv6 next-hop (PBR)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy-based routing (PBR), use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*next-hop-ipv6-address* [{*next-hop-ipv6-address...*}] | **encapsulate l3vpn** *encapsulation-profile* | **peer-address** | **recursive** *next-hop-ipv6-address* | **verify-availability** *next-hop-ipv6-address sequence* **track** *object-number*}
no set ipv6 next-hop {*next-hop-ipv6-address* [{*next-hop-ipv6-address...*}] | **encapsulate l3vpn** *encapsulation-profile* | **peer-address** | **recursive** *next-hop-ipv6-address* | **verify-availability** *next-hop-ipv6-address sequence* **track** *object-number*}

Syntax Description

next-hop-ipv6-address [*next-hop-ipv6-address* ...]	IPv6 global address of the next hop to which packets are sent. The next-hop router must be an adjacent router. The IPv6 address must be specified in hexadecimal using 16-bit values between colons as specified in RFC 2373.
encapsulate	Specifies the encapsulation profile for the next-hop VPN.
l3vpn	Specifies Layer 3 VPN encapsulation.
encapsulation-profile	Encapsulation profile name.
peer-address	Specifies the peer address. This keyword is specific to Border Gateway Protocol (BGP).
recursive *next-hop-ipv6-address*	Specifies the IPv6 address of the recursive next-hop router. • The next-hop IPv6 address must be assigned separately from the recursive next-hop IPv6 address.
verify-availability	Verifies if the next-hop router is reachable.
sequence	Sequence number to insert into the next-hop list. Valid values for the *sequence* argument are from 1 to 65535.
track *object-number*	Sets the next-hop router depending on the state of a tracked object number. Valid values for the *object-number* argument are from 1 to 1000.

Command Default

Packets are not forwarded to a default next hop.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.

Release	Modification
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(2)S	This command was modified. The **recursive** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *next-hop-ipv6-address* argument. You must specify an IPv6 address; an IPv6 link-local address cannot be used because the use of an IPv6 link-local address requires interface context.

The *next-hop-ipv6-address* argument must specify an address that is configured in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is covered by an IPv6 prefix configured on an interface, or an address covered by an IPv6 prefix specified on a directly connected static route.

Examples

The following example shows how to set the next hop to which packets are routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:DB8::1 any
!
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 next-hop 2001:DB8::F
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets are forwarded.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 precedence

To set the precedence value in the IPv6 packet header, use the **set ipv6 precedence** command in route-map configuration mode. To remove the precedence value, use the **no** form of this command.

set ipv6 precedence *precedence-value*
no set ipv6 precedence *precedence-value*

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The way the network gives priority (or some type of expedited handling) to the marked traffic is through the application of weighted fair queueing (WFQ) or weighted random early detection (WRED) at points downstream in the network. Typically, you would set IPv6 precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures that high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as routine and priority to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco high-end Internet quality of service (QoS), IPv6 precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network. For example, IPv6 precedence 2 can be given 90 percent of the bandwidth on output links in the network, and IPv6 precedence 6 can be given 5 percent using the distributed weight fair queueing (DWFQ) implementation on the Versatile Interface Processors (VIPs).

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set route-map** configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the IPv6 precedence value to 5 for packets that pass the route map match:

```
interface serial 0
 ipv6 policy route-map texas
!
route-map cisco1
 match length 68 128
 set ipv6 precedence 5
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the **show bgp ipv6**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. 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*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays the route and more specific routes.
labels	(Optional) Displays Multiprotocol Label Switching (MPLS) label information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	MPLS label information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	MPLS label value advertised for the IPv6 prefix was added to the display.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.2(25)S	6PE multipath information was added to the display.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

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

Examples

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

```
Router# show bgp ipv6 unicast
BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                        0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                           0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1             0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                           0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                           0 3320 1275 559 i
*                   3FFE:C00:E:9::2                        0 1251 1930 559 i
*                   3FFE:3600::A                           0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                           0 293 1275 559 i
*                   3FFE:C00:E:4::2          1             0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                        0 237 3748 1275 559 i
```

The table below describes the significant fields shown in the display.

Table 12: show bgp ipv6 Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6**command, showing information for prefix 3FFE:500::/24:

```
Router# show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  Advertised to peer-groups:
     6BONE
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 673, flapped 429 times in 10:47:45
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 3938, flapped 596 times in 13:03:06, reuse in 00:59:10
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
```

The following is sample output from the **show bgp ipv6**command, showing MPLS label information for an IPv6 prefix that is configured to be an IPv6 edge router using MPLS:

```
Router# show bgp ipv6 unicast 2001:0DB8::/32
BGP routing table entry for 2001:0DB8::/32, version 15
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best, mpls label 17
```

To display the top of the stack label with label switching information, enter the **show bgp ipv6**EXEC command with the **labels** keyword:

```
Router# show bgp ipv6 unicast labels
Network              Next Hop              In tag/Out tag
2001:0DB8::/32       ::FFFF:192.168.99.70   notag/20
```

Note If a prefix has not been advertised to any peer, the display shows "Not advertised to any peer."

The following is sample output from the **show bgp ipv6**command, showing 6PE multipath information. The prefix 4004::/64 is received by BGP from two different peers and therefore two different paths:

```
Router# show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community

To display routes that belong to specified IPv6 Border Gateway Protocol (BGP) communities, use the **show bgp ipv6 community** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community** [*community-number*] [**exact-match**] [{**local-as** | **no-advertise** | **no-export**}]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
community-number	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** and **exact-match** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 community** command provides output similar to the **show ip bgp community**command, except it is IPv6-specific.

Communities are set with the **set community** route-map configuration command. You must enter the numerical communities before the well-known communities. For example, the following string is not valid:

```
Router# show ipv6 bgp community local-as 111:12345
```

Use one of the following strings instead:

```
Router# show ipv6 bgp community 111:12345 local-as
Router# show ipv6 bgp unicast community 111:12345 local-as
```

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

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

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
       Network              Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64      ::                                       0 32768 i
*> 2001:0DB8:0:1:1::/80     ::                                       0 32768 ?
*> 2001:0DB8:0:2::/64       2001:0DB8:0:3::2                            0 2 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:3::2                            0 2 ?
* 2001:0DB8:0:3::1/64       2001:0DB8:0:3::2                            0 2 ?
*>                       ::                                       0 32768 ?
*> 2001:0DB8:0:4::/64       2001:0DB8:0:3::2                            0 2 ?
*> 2001:0DB8:0:5::1/64      ::                                       0 32768 ?
*> 2001:0DB8:0:6::/64       2000:0:0:3::2                            0 2 3 i
*> 2010::/64                ::                                       0 32768 ?
*> 2020::/64                ::                                       0 32768 ?
*> 2030::/64                ::                                       0 32768 ?
*> 2040::/64                ::                                       0 32768 ?
*> 2050::/64                ::                                       0 32768 ?
```

The table below describes the significant fields shown in the display.

Table 13: show bgp ipv6 community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e--Entry originated from the Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
ip bgp-community new-format	Displays BGP communities in the format AA:NN (autonomous system-community number:2-byte number).

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community-list

To display routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list, use the **show bgp ipv6 community-list** command in user EXEC or privileged EXEC mode.

show **bgp** **ipv6** {**unicast** | **multicast**} **community-list** {*numbername*} [**exact-match**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
number	Community list number in the range from 1 to 199.
name	Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast community-list**and **show bgp ipv6 multicast community-list**commands provide output similar to the **show ip bgp community-list**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output of the **show bgp ipv6 community-list** command for community list number 3:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network                 Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64       2001:0DB8:0:3::1                       0 1 i
*> 2001:0DB8:0:1:1::/80     2001:0DB8:0:3::1                       0 1 i
*> 2001:0DB8:0:2::1/64      ::                                  0 32768 i
*> 2001:0DB8:0:2:1::/80     ::                                  0 32768 ?
* 2001:0DB8:0:3::2/64       2001:0DB8:0:3::1                       0 1 ?
*>                        ::                                 0 32768 ?
*> 2001:0DB8:0:4::2/64      ::                                  0 32768 ?
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                       0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                       0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                       0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                       0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                       0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                       0 1 ?
```

The table below describes the significant fields shown in the display.

Table 14: show bgp ipv6 community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Origin codes</td><td>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:
i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command.
e--Entry originated from the Exterior Gateway Protocol (EGP).
?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</td></tr>
<tr><td>Network</td><td>IPv6 address of a network entity.</td></tr>
<tr><td>Next Hop</td><td>IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.</td></tr>
<tr><td>Metric</td><td>The value of the interautonomous system metric. This field is frequently not used.</td></tr>
<tr><td>LocPrf</td><td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td></tr>
<tr><td>Weight</td><td>Weight of the route as set via autonomous system filters.</td></tr>
<tr><td>Path</td><td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td></tr>
</table>

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 dampened-paths

To display IPv6 Border Gateway Protocol (BGP) dampened routes, use the **show bgp ipv6 dampened-paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening dampened-paths**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show bgp ipv6 dampened-paths**and **show bgp ipv6 unicast dampening dampened-paths**commands provide output similar to the **show ip bgp dampened-paths**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 dampened-paths** command:

> **Note** The command output is the same whether or not the **unicast, multicast,**and **dampening** keywords are used. The **unicast**and **dampening**keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening dampened-paths
BGP table version is 12610, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From             Reuse    Path
*d 3FFE:1000::/24   3FFE:C00:E:B::2  00:00:10 237 2839 5609 i
*d 2001:228::/35    3FFE:C00:E:B::2  00:23:30 237 2839 5609 2713 i
```

The table below describes the significant fields shown in the display.

Table 15: show bgp ipv6 dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e--Entry originated from the Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.
Network	Indicates the network to which the route is dampened.
From	IPv6 address of the peer that advertised this path.

Field	Description
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 dampening	Clears IPv6 BGP route dampening information and unsuppresses the suppressed routes.

show bgp ipv6 filter-list

To display routes that conform to a specified IPv6 filter list, use the **show bgp ipv6 filter-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **filter-list** *access-list-number*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
access-list-number	Number of an IPv6 autonomous system path access list. It can be a number from 1 to 199.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 filter-list**command provides output similar to the **show ip bgp filter-list**command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 filter-list** command for IPv6 autonomous system path access list number 1:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast filter-list 1
BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network              Next Hop                          Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64       2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80     2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64       2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64       ::                                         32768  ?
*                           2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64       ::                                         32768  ?
*                           2001:0DB8:0:4::2                         0 2 1 ?
*> 2001:0DB8:0:6::1/64      ::                                         32768  i
*> 2030::/64                2001:0DB8:0:4::2                         0 1
*> 2040::/64                2001:0DB8:0:4::2                         0 2 1 ?
*> 2050::/64                2001:0DB8:0:4::2                         0 2 1 ?
```

The table below describes the significant fields shown in the display.

Table 16: show bgp ipv6 filter-list Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented any time the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i--The entry was originated with the IGP and advertised with a **network** router configuration command. • e--The route originated with EGP. • ?--The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

Related Commands

Command	Description
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 flap-statistics

To display IPv6 Border Gateway Protocol (BGP) flap statistics , use the **show bgp ipv6 flap-statistics** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening flap-statistics** [**regexp** *regular-expression* | **quote-regexp** *regular-expression* | **filter-list** *list* | *ipv6-prefix*/*prefix-length* [**longer-prefix**]]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.
regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list *list*	(Optional) Displays flap statistics for all the paths that pass the access list.
ipv6-prefix	(Optional) Displays flap statistics for a single entry at this IPv6 network number.
/ipv6-prefix	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast dampening flap-statistics** and **show bgp ipv6 multicast dampening flap-statistics** commands provide output similar to the **show ip bgp flap-statistics** command, except they are IPv6-specific.

If no arguments or keywords are specified, the router displays flap statistics for all routes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the**unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the**unicast** or**multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 flap-statistic s** command without arguments or keywords:

Note The output is the same whether or not the **unicast**, **multicast** and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening flap-statistics

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Flaps Duration Reuse    Path
*d 2001:200::/35    3FFE:1100:0:CC00::1
                                    12145 10:09:15 00:57:10 1849 2914 4697 2500
*  2001:218::/35    2001:0DB8:0:F004::1
                                    2     00:03:44          3462 4697
```

The table below describes the significant fields shown in the display.

Table 17: show bgp ipv6 flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IPv6 address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 flap-statistics	Clears IPv6 BGP flap statistics.
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 inconsistent-as

To display IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems, use the **show bgp ipv6 inconsistent-as** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **inconsistent-as**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast inconsistent-as**and **show bgp ipv6 multicast inconsistent-as**commands provide output similar to the **show ip bgp inconsistent-as** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 inconsistent-as** command:

Note

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast inconsistent-as
BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                        0 1251 4270 10318 ?
*                   3FFE:3600::A                           0 3462 6175 ?
*                   3FFE:700:20:1::11                      0 293 6175 ?
```

The table below describes the significant fields shown in the display.

Table 18: show bgp ipv6 inconsistent-as Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 labels

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 labels**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **labels**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Usage Guidelines

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

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

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast labels
Network                     Next Hop        In label/Out label
2001:1:101::1/128           ::FFFF:172.17.1.1  nolabel/19
2001:3:101::1/128           ::FFFF:172.25.8.8  nolabel/19
```

The table below describes the significant fields shown in the display.

Table 19: show bgp ipv6 labels Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
In label/Out label	IPv6 BGP connections.

IPv6 Commands: show bgp ipv6 ne to show ipv6 cef sw

show bgp ipv6 neighbors

To display information about IPv6 Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **neighbors** [*ipv6-address*] [{**received-routes** | **routes** | **flap-statistics** | **advertised-routes** | **paths** *regular-expression* | **dampened-routes**}]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-address	(Optional) Address of the IPv6 BGP-speaking neighbor. If you omit this argument, all IPv6 neighbors are displayed. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes received and accepted. This is a subset of the output from the **received-routes** keyword.
flap-statistics	(Optional) Displays flap statistics for the routes learned from the neighbor.
advertised-routes	(Optional) Displays all the routes the networking device advertised to the neighbor.
paths *regular-expression*	(Optional) Regular expression used to match the paths received.
dampened-routes	(Optional) Displays the dampened routes to the neighbor at the IP address specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	IPv6 capability information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.

Release	Modification
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show bgp ipv6 unicast neighbors**and **show bgp ipv6 multicast neighbors**commands provide output similar to the **show ip bgp neighbors** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

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

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
 Member of peer-group 6BONE for session parameters
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  6BONE peer-group member
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
```

```
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

The following is sample output from the **show bgp ipv6 neighbors** command when the router is configured to allow IPv6 traffic to be transported across an IPv4 Multiprotocol Label Switching (MPLS) network (Cisco 6PE) without any software or hardware upgrade in the IPv4 core infrastructure. A new neighbor capability is added to show that an MPLS label is assigned for each IPv6 address prefix to be advertised. 6PE uses multiprotocol BGP to provide the reachability information for the 6PE routers across the IPv4 network so that the neighbor addresses are IPv4.

```
Router# show bgp ipv6 unicast neighbors
BGP neighbor is 10.11.11.1,  remote AS 65000, internal link
  BGP version 4, remote router ID 10.11.11.1
  BGP state = Established, up for 04:00:53
  Last read 00:00:02, hold time is 15, keepalive interval is 5 seconds
  Configured hold time is 15, keepalive interval is 10 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv6 Unicast: advertised and received
    ipv6 MPLS Label capability: advertised and received
  Received 67068 messages, 1 notifications, 0 in queue
  Sent 67110 messages, 16 notifications, 0 in queue
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv6 Unicast
  BGP table version 91, neighbor version 91
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Sending Prefix & Label
  4 accepted prefixes consume 288 bytes
  Prefix advertised 90, suppressed 0, withdrawn 2
  Number of NLRIs in the update sent: max 3, min 0
  Connections established 26; dropped 25
  Last reset 04:01:20, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.11.11.1, Foreign port: 11003
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1429F084):
```

```
Timer          Starts    Wakeups            Next
Retrans          2971         77             0x0
TimeWait            0          0             0x0
AckHold          2894       1503             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss:  803218558  snduna:  803273755  sndnxt:  803273755     sndwnd:  16289
irs: 4123967590  rcvnxt: 4124022787  rcvwnd:      16289  delrcvwnd:     95
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 32 ms, maxRTT: 408 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
Datagrams (max data segment is 536 bytes):
Rcvd: 4531 (out of order: 0), with data: 2895, total data bytes: 55215
Sent: 4577 (retransmit: 77, fastretransmit: 0), with data: 2894, total data
bytes: 55215
```

The table below describes the significant fields shown in the display.

Table 20: show bgp ipv6 neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
remote AS	Autonomous system of the neighbor.
internal link	Indicates that this peer is an interior Border Gateway Protocol (iBGP) peer.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
BGP state	Internal state of this BGP connection.
up for	Amount of time that the underlying TCP connection has been in existence.
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.

Field	Description
Address family IPv6 Unicast	Indicates that BGP peers are exchanging IPv6 reachability information.
ipv6 MPLS Label capability	Indicates that MPLS labels are being assigned to IPv6 address prefixes.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer.
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.
advertisement runs	Value of the minimum advertisement interval.
For address family	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Route refresh request	Number of route refresh requests sent and received from this neighbor.
Community attribute (not shown in sample output)	Appears if the neighbor send-community command is configured for this neighbor.
Inbound path policy (not shown in sample output)	Indicates whether an inbound filter list or route map is configured.
Outbound path policy (not shown in sample output)	Indicates whether an outbound filter list, route map, or unsuppress map is configured.
bgp-in (not shown in sample output)	Name of the inbound update prefix filter list for the IPv6 unicast address family.
aggregate (not shown in sample output)	Name of the outbound update prefix filter list for the IPv6 unicast address family.
uni-out (not shown in sample output)	Name of the outbound route map for the IPv6 unicast address family.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.

Field	Description
history paths (not shown in sample output)	Number of path entries held to remember history.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time (in hours:minutes:seconds) since this peering session was last reset.
Connection state	State of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of the local router, plus the port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table that displays the number of starts and wakeups for each timer.
iss	Initial send sequence number.
snduna	Last send sequence number for which the local host sent but has not received an acknowledgment.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrecvwnd	Delayed receive window--data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout (in milliseconds).
RTTO	Round-trip timeout (in milliseconds).
RTV	Variance of the round-trip time (in milliseconds).
KRTT	New round-trip timeout (in milliseconds) using the Karn algorithm. This field separately tracks the round-trip time of packets that have been re-sent.

Field	Description
minRTT	Smallest recorded round-trip timeout (in milliseconds) with hard wire value used for calculation.
maxRTT	Largest recorded round-trip timeout (in milliseconds).
ACK hold	Time (in milliseconds) the local host will delay an acknowledgment in order to "piggyback" data on it.
Flags	IP precedence of the BGP packets.
Datagrams: Rcvd	Number of update packets received from neighbor.
with data	Number of update packets received with data.
total data bytes	Total number of bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show bgp ipv6 neighbors** command with the **advertised-routes** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                        0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                        0 3748 4697 i
```

The following is sample output from the **show bgp ipv6 neighbors** command with the **routes** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                      0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                      0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                      0 293 1275 3748 i
```

The table below describes the significant fields shown in the display.

Table 21: show bgp ipv6 neighbors advertised-routes and routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6 neighbors** command with the **paths** keyword:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
```

```
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

Note The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

The table below describes the significant fields shown in the display.

Table 22: show bgp ipv6 neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

The following sample output from the **show bgp ipv6 neighbors** command shows the dampened routes for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 dampened-routes
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From              Reuse    Path
*d 3FFE:8030::/28   3FFE:700:20:1::11 00:24:20 293 1275 559 8933 i
```

The following sample output from the **show bgp ipv6 neighbors** command shows the flap statistics for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 flap-statistics
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From             Flaps Duration Reuse    Path
*d 2001:668::/35    3FFE:700:20:1:: 4923  2d12h    00:59:50 293 1849 3257
*d 3FFE::/24        3FFE:700:20:1:: 4799  2d12h    00:59:30 293 1849 5609 4554
*d 3FFE:8030::/28   3FFE:700:20:1:: 95    11:48:24 00:23:20 293 1275 559 8933
```

The following sample output from the **show bgp ipv6 neighbors** command shows the received routes for IPv6 address 2000:0:0:4::2:

```
Router#
show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
Network                Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                        0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                        0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                        0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                        0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                        0 2 ?
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

show bgp ipv6 paths

To display all the IPv6 Border Gateway Protocol (BGP) paths in the database, use the **show bgp ipv6 paths**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **paths** *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
regular-expression	Regular expression that is used to match the received paths in the database.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast paths**and **show bgp ipv6 multicast paths**commands provide output similar to the **show ip bgp paths** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

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

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast paths
Address     Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

The table below describes the significant fields shown in the display.

Table 23: show bgp ipv6 paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show bgp ipv6 peer-group

To display information about Border Gateway Protocol (BGP) peer groups, use the **show bgp ipv6 peer-group**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **peer-group** [*name*]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	(Optional) Peer group name.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The unicast and **multicast**keywords were added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Usage Guidelines

If a user does not specify a peer group name, then all BGP peer groups will be displayed.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 peer-group**command:

```
Router# show bgp ipv6 unicast peer-group
BGP peer-group is external-peerings,  remote AS 20
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds
 For address family:IPv6 Unicast
  BGP neighbor is external-peerings, peer-group external, members:
  1::1
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent:max 0, min 0
```

The table below describes the significant fields shown in the display.

Table 24: show bgp ipv6 peer-group Field Descriptions

Field	Description
BGP peer-group is	Type of BGP peer group.
remote AS	Autonomous system of the peer group.
BGP version	BGP version being used to communicate with the remote router.
For address family: IPv4 Unicast	IPv6 unicast-specific properties of this neighbor.

show bgp ipv6 prefix-list

To display routes that match a prefix list, use the **show bgp ipv6 prefix-list**command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **prefix-list** *name*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	The specified prefix list.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The unicast and **multicast**keywords were added.

Usage Guidelines

The specified prefix list must be an IPv6 prefix list, which is similar in format to an IPv4 prefix list.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 prefix-list**command:

```
Router# show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

The table below describes the significant fields shown in the display.

Table 25: show bgp ipv6 prefix-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 quote-regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression as a quoted string of characters, use the **show bgp ipv6 quote-regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **quote-regexp** *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
regular-expression	Regular expression that is used to match the BGP autonomous system paths.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast quote-regexp**and **show bgp ipv6 multicast quote-regexp**commands provide output similar to the **show ip bgp quote-regexp** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 quote-regexp** command that shows paths beginning with 33 or containing 293:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

Note The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

The table below describes the significant fields shown in the display.

Table 26: show bgp ipv6 quote-regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
show bgp ipv6 regexp	Displays IPv6 BGP routes matching the autonomous system path regular expression.
show ip bgp regexp	Displays routes matching the regular expression.

show bgp ipv6 regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression, use the **show bgp ipv6 regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **regexp** *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
regular-expression	Regular expression that is used to match the BGP autonomous system paths.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast**keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show bgp ipv6 unicast regexp**and **show bgp ipv6 multicast regexp**commands provide output similar to the **show ip bgp regexp**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 regexp** command that shows paths beginning with 33 or containing 293:

> **Note** The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

> **Note** The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

The table below describes the significant fields shown in the display.

Table 27: show bgp ipv6 regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 route-map

To display IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table, use the **show bgp ipv6 route-map** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **route-map** *name*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
name	A specified route map to match.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The unicast and **multicast**keywords were added.

Usage Guidelines

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 route-map**command for a route map named rmap:

```
Router# show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1         0    100     50 ?
*>i543::/64         2001:0DB8:101::1         0    100     50 ?
```

The table below describes the significant fields shown in the display.

Table 28: show bgp ipv6 route-map Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session. • r --A RIB failure has occurred. • S--The route map is stale.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 summary

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 summary** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **summary**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

The **show bgp ipv6 unicast summary**and **show bgp ipv6 multicast summary**commands provide output similar to the **show ip bgp summary**command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast**keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

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

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Device# show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2  4    200    6869     6882        0    0     0  06:25:24  Active
```

The table below describes the significant fields shown in the display.

Table 29: show bgp ipv6 summary Field Descriptions

Field	Description
BGP device identifier	IP address of the networking device.
BGP table version	Internal version number of the BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
Neighbor	IPv6 address of a neighbor.
V	BGP version number spoken to that neighbor.
AS	Autonomous system.
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.
Up/Down	The length of time that the BGP session has been in state Established, or the current state if it is not Established.

Field	Description
State/PfxRcd	Current state of the BGP session/the number of prefixes the device has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP TCP connection using BGP soft reconfiguration.
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor shutdown	Disables a neighbor or peer group.

show bgp vpnv6 unicast

To display Virtual Private Network Version 6 (VPNv6) unicast entries in a Border Gateway Protocol (BGP) table, use the **show bgp vpnv6 unicast** command in user EXEC or privileged EXEC mode.

show bgp vpnv6 unicast [{**all** | **vrf** [*vrf-name*]}]

Syntax Description

all	(Optional) Displays all entries in a BGP table.
vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for IPv4 or IPv6 address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

BGP is used for distributing VPN IPv6 routing information in the VPN backbone. The local routes placed in the BGP routing table on an egress provider edge (PE) router are distributed to other PE routers.

Examples

The following examples shows BGP entries from all of the customer-specific IPv6 routing tables:

```
Router# show bgp vpnv6 unicast all

Network                  Next Hop              Metric LocPrf    Weight Path
Route Distinguisher: 100:1
*  2001:100:1:1000::/56   2001:100:1:1000::72a    0               0     200 ?
*                         ::                 0                      32768 ?
*  i2001:100:1:2000::/56  ::FFFF:200.10.10.1
Route Distinguisher: 200:1
*  2001:100:2:1000::/56   ::               0                        32768 ?
*  2001:100:2:2000::/56   ::FFFF:200.10.10.1      0                  32768 ?
```

The table below describes the significant fields shown in the displays.

Table 30: show bgp vpnv6 unicast Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
Loc Prf	Local preference value as configured with the **set local-preference** command.
Weight	Weight of the route as set through autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i—The entry was originated with the IGP and advertised with a network router configuration command. • e—The route originated with EGP. • ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.
Route Distinguisher	Specifies the VRF instance.

Related Commands

Command	Description
show bgp vpnv6 multicast	Displays VPNv6 multicast entries in a BGP table.

show erm statistics

To display the Embedded Resource Manager (ERM) Forwarding Information Base (FIB) ternary content addressable memory (TCAM) exception status for IPv4, IPv6, and Multiprotocol Label Switching (MPLS) protocols, use the **show erm statistics** command in privileged EXEC mode.

show erm statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The IPv4, IPv6, and MPLS exception state displays FALSE when the protocol is not under the exception or displays TRUE when the protocol is under the exception.

Examples

This example shows how to display FIB TCAM exception status for IPv4, IPv6, and MPLS protocols:

```
Router#
show erm statistics
#IPv4 excep notified     = 0
#IPv6 excep notified     = 0
#MPLS excep notified     = 0
#IPv4 reloads done       = 0
#IPv6 reloads done       = 0
#MPLS reloads done       = 0
Current IPv4 excep state = FALSE
Current IPv6 excep state = FALSE
Current MPLS excep state = FALSE
#Timer expired           = 0
#of erm msgs             = 1
```

The table below describes the significant fields shown in the display.

Table 31: show erm statistics Field Descriptions

Field	Description
... excep notified	The number of exceptions for each protocol.
... reloads done	The number of reloads for each protocol.
...Current *protocol* exception state	The current exception status of each protocol.
#of erm msgs	The number of ERM messages sent.

Related Commands

Command	Description
mls erm priority	Assigns the priorities to define an order in which protocols attempt to recover from the exception status.

show fm ipv6 pbr all

To display IPv6 policy-based routing (PBR) value mask results (VMRs), use the **show fm ipv6 pbr all** command in privileged EXEC mode.

show fm ipv6 pbr all

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **show fm ipv6 pbr all** command shows the IPv6 PBR VMRs for all interfaces on which IPv6 PBR is configured.

show fm ipv6 pbr interface

To displays the IPv6 policy-based routing (PBR) value mask results (VMRs) on a specified interface, use the **show fm ipv6 pbr interface** command in privileged EXEC mode.

show fm ipv6 pbr interface interface *type number*

Syntax Description

interface *type number*	Specified interface for which PBR VMR information will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **show fm ipv6 pbr interface** command shows the IPv6 PBR VMRs for a specified interface.

show fm ipv6 traffic-filter

To display the IPv6 information, use the **show fm ipv6 traffic-filter** command in privileged EXEC mode .

show fm ipv6 traffic-filter {**all** | **interface** *type number*}

Syntax Description

all	Displays IPv6 traffic filter information for all interfaces.
interface *type*	Displays IPv6 traffic filter information for the specified interface; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, **ge-wan**and **vlan**
number	Module and port number; see the "Usage Guidelines" section for valid values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to display the IPv6 information for a specific interface:

```
Router# show fm ipv6 traffic-filter interface vlan 50

-------------------------------------------------------------------------------
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
===============================================================================
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
```

```
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+----+-+---------------------------------------+---------------------------------------+---+---+-+-----+----+------+
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
+----+-+---------------------------------------+---------------------------------------+---+---+-+-----+----+------+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
10 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
11 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
12 V
:: :: 58 --- - ----L ---- Shorte
M
```

```
:: :: 255 0
TM_PERMIT_RESULT
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
14 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
15 V
:: :: 0 --- - ----L ---- Shorte
M
:: :: 0 0
TM_L3_DENY_RESULT
Router#
```

This example shows how to display the IPv6 information for all interfaces:

```
Router# show fm ipv6 traffic-filter
 all

-----------------------------------------------------------------------------
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
=============================================================================
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+----+-+-----------------------------------+-------------------------------------+---+---+-+-----+----+------+
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
+----+-+-----------------------------------+-------------------------------------+---+---+-+-----+----+------+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
```

```
5 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: :: 0 -F- - ----L ---- Shorte
M
:: :: 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
8 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
9 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
10 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
.
. Output is truncated
.
Interface(s) using this IPv6 Ingress Traffic Filter:
Vl50,
```

show fm raguard

To display the interfaces configured with router advertisement (RA) guard, use the **show fm raguard**command in privileged EXEC mode.

show fm raguard

Syntax Description

This command has no arguments or keywords.

Command Default

RA guard interface information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.

Usage Guidelines

Use the **show fm raguard** command to verify information about interfaces that are configured with RA guard.

Examples

The following example enables the display of interfaces configured with IPv6 RA guard:

```
Router# show fm raguard
------------------------------------------------------------------------------
 IPV6 RA GUARD in Ingress direction is configured on following interfaces
==============================================================================
Interface: Port-channel23
Interface: GigabitEthernet4/6
```

The table below describes the significant fields shown in the display.

Table 32: show fm raguard Field Descriptions

Field	Description
IPV6 RA GUARD in Ingress direction is configured on following interfaces	Displays the interfaces configured with IPv6 RA guard.

show ipv6 access-list

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

show ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of access list.

Command Default

All IPv6 access lists are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list**command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

Table 33: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.
tcptraffic (8 matches)	The name of the reflexive IPv6 access list and the number of matches for the access list. The **clear ipv6 access-list** privileged EXEC command resets the IPv6 access list match counters.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.

Field	Description
11000	The ephemeral source port number for the outgoing connection.
timeout 300	The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.
(time left 243)	The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

show ipv6 cef

To display entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef** command in user EXEC or privileged EXEC mode.

Privileged EXEC Mode

User EXEC Mode

Syntax Description

ipv6-prefix	(Optional) 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*	(Optional) The IPv6 network assigned to the interface and the length of the IPv6 prefix. • The *ipv6-prefix* must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The *prefix-length* is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays FIB information for more specific destinations.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
platform	(Optional) Displays platform-specific Cisco Express Forwarding data.
detail	(Optional) Displays detailed FIB entry information.
internal	(Optional) Displays internal FIB entry information.
checksum	(Optional) Displays FIB entry checksums.
dependents	(Optional) Displays dependents of the selected prefix.
similar-prefixes	(Optional) Displays FIB information for prefixes that are similar to one another.
epoch	(Optional) Displays the basic FIB entries filtered by epoch number.
summary	(Optional) Displays the summary of events log.
new	(Optional) Displays new events since the last show operation was performed.
within *minutes*	(Optional) Displays events within the specified time, in minutes. The range is from 1 to 4294967295.
prefix-statistics	(Optional) Displays nonzero prefix statistics.

Command Default

If no keyword or argument is specified, information about all FIB entries is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *interface-type* and *interface-number* arguments and the **longer-prefixes** and **detail** keywords were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	This command was modified. The **dependents**, **events**, **internal, new, platform**, **similar-prefixes** and **within** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **show ipv6 cef**command is similar to the **show ip cef**command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 cef**command when no keywords or arguments are entered:

```
Router# show ipv6 cef
Global IPv6 CEF Table
12 prefixes
2FFE::3/128
  Receive
2FFE::/64
  attached to POS3/1
3FFE::/64
  nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1
  nexthop FE80::xxxx:7DFF:FE8D:A840 FastEthernet1/0
3FFE:zz::3/128
  Receive
3FFE:zz::/64
  attached to FastEthernet1/0
3FFE:rr::3/128
  Receive
3FFE:rr::/64
  attached to FastEthernet1/1
3FFE:pp::3/128
  Receive
3FFE:pp::/64
  attached to FastEthernet1/2
3FFE:nnnn:2222::/64
```

```
  nexthop::POS3/1
3FFE:ssss::/64
  recursive via 2FFE::2 POS3/1
FE80::/64
  Receive
```

The following is sample output from the **show ipv6 cef**command showing 6PE multipath information:

```
Router# show ipv6 cef
Global IPv6 CEF Table
12 prefixes
.
.
.
nexthop 10.1.1.3 Ethernet0/0 label 25 16
4004::/64
  nexthop 10.1.1.3 Ethernet0/0 label 27 16
  nexthop 10.1.1.3 Ethernet0/0 label 26 18
```

The table below describes the significant fields shown in the displays.

Table 34: show ipv6 cef Field Descriptions

Field	Description
12 prefixes	Indicates the total number of IPv6 prefixes in the Cisco Express Forwarding table.
2FFE::3/128	Indicates the IPv6 prefix of the remote network.
Receive	Indicates that this IPv6 prefix is local to the router.
3FFE::/64 nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1 nexthop FE80::xxxx:7DFF:FE8D:A840 FastEthernet1/0	Indicates that IPv6 prefix 3FFE::/64 is reachable through these next hop addresses and interfaces. • Multiple next-hop entries are shown for IPv6 prefixes that have load sharing.
attached to FastEthernet1/0	Indicates that this IPv6 prefix is a connected network on Fast Ethernet interface 1/0.
recursive via 2FFE::2 POS3/1	Indicates that this IPv6 prefix uses the same forwarding information as 2FFE::2 POS3/1.

The following is sample output from the **show ipv6 cef detail** command for Fast Ethernet interface 1/0:

```
Router# show ipv6 cef fastethernet 1/0 detail
IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:zz::/64
  attached to FastEthernet1/0
3FFE:rr::/64
  attached to FastEthernet1/1
```

The fields in the are self-explanatory.

The following is sample output from the **show ipv6 cef longer-prefixes**command for the IPv6 prefix 3FFE:xxxx:20:1::12/128. The fields in the display are self-explanatory.

```
Router# show ipv6 cef 3FFE:xxxx:20:1::12/128 longer-prefixes
IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:xxxx:20:1::12/128 Receive
  Receive
3FFE:xxxx:20:1::/64 Attached, Connected
     attached to Tunnel81
```

The following is sample output from the **show ipv6 cef detail**command showing 6PE multipath information. The prefix 4004::/64 is received by the Border Gateway Protocol (BGP) from two different peers and therefore two different paths.

```
Router# show ipv6 cef detail
IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, version 20, 0 resets
 Database epoch:0 (20 entries at this epoch)
.
.
.
4004::/64, epoch 0, per-destination sharing
  recursive via 172.11.11.1 label 27
    nexthop 10.1.1.3 Ethernet0/0 label 16
  recursive via 172.30.30.1 label 26
    nexthop 10.1.1.3 Ethernet0/0 label 18
```

The fields in the display are self-explanatory.

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

```
Router# show ipv6 cef internal
IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
14 prefixes tableid 0
table version 17
root 6283F5D0
.
.
.
BEEF:20::/64 RIBfib  <=====================entry with two mpls path
 Using loadinfo 0x62A75194
  loadinfo ptr 62A75194 flags 0000 next hash  = 0
  refcount 3 path list ptr 0x00000000
  hashes :-
      62335678  drop adjacency
     .
     .
     .
  path list pointer 62370FA0
    2 paths -
     Nexthop  path_pointer 6236E420 traffic share 1 path_list pointer 62370FA0
     nexthop ::FFFF:172.12.12.1
     next_hop_len 0 adjacency pointer 62335678
     Nexthop  path_pointer 6236E480 traffic share 1 path_list pointer 62370FA0
     nexthop ::FFFF:172.14.14.1
```

```
     next_hop_len 0 adjacency pointer 62335678
    refcount 2
    1 loadinfos -
     loadinfo ptr 62A75194 flags 0000 next hash  = 0
     refcount 3 path list ptr 0x00000000
     hashes :-
       62335678  drop adjacency
      .
      .
      .
  tag information
    local tag: exp-null
    rewrites :-
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
       Fa0/1, 10.2.1.1, tags imposed: {32}
       Fa1/0, 10.1.1.3, tags imposed: {25}
FE80::/10 Receive, RIBfib
  Receive
FF00::/8 Receive, RIBfib
  Receive
```

The table above and the table below describe the significant fields shown in displays.

Table 35: show ipv6 cef internal Field Descriptions

Field	Description
Slow processing intvl	Displays the slow processing interval, in seconds.
backoff level current/max	Displays the backoff level in the ratio current to the maximum backoff value.
unresolved prefixes	Displays the total number of unresolved prefixes.
requiring adjacency update	Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution.
prefixes	Total number of prefixes in the IPv6 Cisco Express Forwarding default table.
tableid	ID of the IPv6 Cisco Express Forwarding default table.
table version	Version of the IPv6 Cisco Express Forwarding default table.
root	Root number of the IPv6 Cisco Express Forwarding default table.
Using loadinfo	Current load information
loadinfo ptr	Load information pointer.
flags	Total number of flags.

Field	Description
next hash	Next hash value.
refcount 3 path list ptr	Location of the refcount 3 path list pointer.
hashes	Total number of hashes.
Nexthop path_pointer	Location of the next hop path pointer.
path_list pointer	Location of the path list pointer.
refcount	Location of the reference counter.
loadinfo ptr	Location of the load information pointer.

The following is sample output from the **show ipv6 cef internal** command showing 6PE multipath information. The fields in the display are self-explanatory.

```
Router# show ipv6 cef internal
4004::/64, version 15, epoch 0, RIB, refcount 3, per-destination sharing
  sources:RIB
  feature space:
   IPRM:0x00028000
  path 01A53DA0, path list 01A4F2E0, share 0, flags recursive, resolved
  ifnums:(none)
   path_list contains no resolved destination(s). HW IPv4 notified.
  recursive via 172.11.11.1 label 27, fib 01A6CCA0, 1 terminal fib
    path 01A540B0, path list 01A4F5F0, share 1, flags nexthop
    ifnums:(none)
     path_list contains no resolved destination(s). HW IPv4 notified.
    nexthop 10.1.1.3 Ethernet0/0 label 16, mask /0, adjacency IP adj out of
Ethernet0/0, addr 10.1.1.3 01DE9FB0
  path 01A53D30, path list 01A4F2E0, share 0, flags recursive, resolved
  ifnums:(none)
   path_list contains no resolved destination(s). HW IPv4 notified.
  recursive via 172.30.30.1 label 26, fib 01A6CBD0, 1 terminal fib
    path 01A540B0, path list 01A4F5F0, share 1, flags nexthop
    ifnums:(none)
     path_list contains no resolved destination(s). HW IPv4 notified.
    nexthop 10.1.1.3 Ethernet0/0 label 18, mask /0, adjacency IP adj out of
Ethernet0/0, addr 10.1.1.4 01DE9FB0
  output chain:
    loadinfo 01A47520, per-session, flags 0011, 2 locks
    flags:Per-session, for-mpls-not-at-eos
    16 hash buckets
      <0  > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <1  > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <2  > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <3  > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
      <4  > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
.
.
.
      <15 > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
```

The following is sample output from the **show ipv6 cef**command, showing information about the Multiprotocol Label Switching (MPLS) labels associated with the FIB table entries for an IPv6 prefix that is configured to be a Cisco 6PE router using MPLS to transport IPv6 traffic over an IPv4 network.

To display label information from the Cisco Express Forwarding table, enter the **show ipv6 cef**command with an IPv6 prefix. The fields in the display are self-explanatory.

```
Router# show ipv6 cef 2001:0DB8::/32
2001:0DB8::/32
      nexthop ::FFFF:192.168.99.70
      fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
```

Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA,12.2(33)SXH, 12.4(20)T, and Later Releases

The sample output in the following commands was reformatted with the implementation of Cisco Express Forwarding enhancements. The information in the output is the same as it was before the enhancements.

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

```
Router# show ipv6 cef internal
IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 0 (20 entries at this epoch)
2001:1:12::/64, epoch 0, RIB, refcount 3
  sources: RIB
  feature space:
   MFI: path extension list empty
   IPRM: 0x00038000
   IPV6 adj out of POS1/0 635BAFE0
  path 633A9A18, path list 633A732C, share 1, type attached nexthop
  ifnums: (none)
   path_list contains at least one resolved destination(s). HW IPv6 notified.
  nexthop FE80::205:DCFF:FE26:4800 POS1/0, adjacency IPV6 adj out of POS1/0 635BAFE0
  output chain: IPV6 adj out of POS1/0 635BAFE0
```

The fields in the display are self-explanatory.

The following is sample output from the **show ipv6 cef** *ipv6-prefix* **/** *prefix-length* **internal** command:

```
Router# show ipv6 cef 2001:2:25::/64 internal
2001:2:25::/64 RIBfib
 Using cached adjacency 0x629E1CE0
  path list pointer 62A2C310
    1 path -
     Nexthop  path_pointer 62A297B0 traffic share 1 path_list pointer 62A2C310
     nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1
     next_hop_len 0 adjacency pointer 629E1CE0
    refcount 10
    no loadinfo
```

The following is sample output from the **show ipv6 cef detail** command. The fields in the display are self-explanatory.

```
Router# show ipv6 cef detail
IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 0 (20 entries at this epoch)
2001:1:12::/64, epoch 0
  nexthop FE80::205:DCFF:FE26:4800 POS1/0
2001:2:13::/64, epoch 0, flags attached, connected
  attached to POS1/0
2001:2:13::2/128, epoch 0, flags receive
```

The following is sample output from the **show ipv6 cef epoch** command. The fields in the display are self-explanatory.

```
Router# show ipv6 cef epoch
Table: Default
 Database epoch: 1 (2 entries at this epoch)
```

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef adjacency	Displays Cisco Express Forwarding for IPv6 recursive and direct prefixes resolved through an adjacency.
show ipv6 route	Displays IPv6 router advertisement information received from onlink routers.

show ipv6 cef adjacency

To display Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding v6 recursive and direct prefixes resolved through an adjacency, use the **show ipv6 cef adjacency** command in user EXEC or privileged EXEC mode.

show ipv6 cef adjacency *interface-type interface-number ipv6-address* [{**detail** | **internal** | **samecable**}] [**platform** [{**detail** | **internal** | **samecable**}]] [**source** [{**internal** | **epoch** *epoch-number* [{**internal** | **samecable** | **platform** [{**detail** | **internal** | **samecable**}]}]}]] [**epoch** *epoch-number* [{**internal** | **samecable** | **platform** [{**detail** | **internal** | **samecable**}]}]]

Syntax Description

interface-type	Interface type for which to display Cisco Express Forwarding adjacency information.
interface-number	Interface number for which to display adjacency information.
ipv6-address	Next-hop IPv6 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.
detail	(Optional) Displays detailed information for each CEFv6 adjacency type entry.
internal	(Optional) Displays data for adjacency type entries.
samecable	(Optional) Displays the connected (up) interface for adjacency type entries.
platform	(Optional) Displays platform-specific adjacency information.
source	(Optional) Displays source-specific adjacency information.
epoch *epoch-number*	(Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255.
discard	Displays discard adjacency information. Sets up for loopback interfaces. Loopback IPv6 addresses are receive entries in the FIB table.
drop	Displays drop adjacency information. Packets forwarded to this adjacency are dropped.
glean	Displays glean adjacency information. Represents destinations on a connected interface for which no Address Resolution Protocol (ARP) cache entry exists.
null	Displays null adjacency information. Formed for the null 0 interface. Packets forwarded to this adjacency are dropped.
punt	Displays punt adjacency information. Represents destinations that cannot be switched in the normal path and that are punted to the next fastest switching vector.
adj-null	Displays null adjacency information.
checksum	(Optional) Displays FIB entry checksums.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	This command was modified. The **internal**, **samecable**, **platform**, and **source** keywords were added.
12.2(28)SB	This command was modified. The **null** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show ipv6 cef adjacency** command is similar to the **show ip cef adjacency** command, except that it is IPv6 specific.

This command shows all prefixes resolved through a regular next-hop adjacency or through a special adjacency type such as discard, drop, glean, null, and punt. An adjacency is a node that can be reached by one Layer 2 hop.

Examples

The following is sample output from the **show ipv6 cef adjacency** command when the **glean** type is specified:

```
Router# show ipv6 cef adjacency glean
Prefix              Next Hop              Interface
3FFE:xxxx::/24       attached              Ethernet1
2002::/16           3FFE:xxxx::1           Ethernet1
```

The following is sample output from the **show ipv6 cef adjacency drop** command with **detail** specified:

```
Router# show ipv6 cef adjacency
 fastethernet
 0/1 drop detail
IPv6 CEF is enabled and running
IPv6 CEF default table
12 prefixes
```

The following sample output shows the direct IPv6 prefix when next-hop Ethernet interface 1 is specified:

```
Router# show ipv6 cef adjacency ethernet 1 3FFE:xxxx::250:8BFF:FEE8:F800
Prefix                                       Next Hop             Interface
3FFE:xxxx::250:8BFF:FEE8:F800/128            2002::/16          Ethernet1
```

The table below describes the fields shown in the display.

Table 36: show ipv6 cef adjacency Field Descriptions

Field	Description
Prefix	Destination IPv6 prefix.
Next Hop	Next-hop IPv6 address.
Interface	Next-hop interface.

Related Commands

Command	Description
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ipv6 cef events

To display IPv6 Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) and adjacency events, use the **show ipv6 cef events** command in privileged EXEC mode.

show ipv6 cef events [{[*ipv6-prefix*] [{**new** | **within** *minutes*}] [**detail**] | **summary**}]

Syntax Description

ipv6-prefix	(Optional) 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.
new	(Optional) Displays new events since the last show operation was performed.
within *minutes*	(Optional) Displays events within the specified time, in minutes. The range is from 1 to 4294967295.
minutes	(Optional) Time in minutes. The range is from 1 to 4294967295.
detail	(Optional) Displays detailed FIB entry information.
summary	(Optional) Displays the summary of event log.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **show ipv6 cef events** command is similar to the **show ip cef events** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 cef events** command when used without any arguments or keywords:

```
Router# show ipv6 cef events
*Apr 23 07:49:40.861: [v6:Default] *::*/*             Allocated FIB table       [OK]
*Apr 23 07:49:40.861: [v6:Default] *::*/*'00          Add source Default table  [OK]
```

```
*Apr 23 07:49:40.861: [v6:Default] ::/0'00            FIB add src DRH (ins)     [OK]
*Apr 23 07:49:40.861: [v6:Default] *::*/*'00          New FIB table             [OK]\
```

The table below describes the significant fields shown in the display.

Table 37: show ipv6 cef events Field Descriptions

Field	Description
[v6:Default]	Type of VRF table for this event entry.
::/*'00	IPv6 prefix.
[OK]	Cisco Express Forwarding processed event.

Related Commands

Command	Description
show ip cef events	Displays all recorded Cisco Express Forwarding FIB and adjacency events.
show ipv6 cef	Displays entries in the IPv6 FIB.

show ipv6 cef exact-route

To display the exact route for a source-destination IPv6 address pair, use the **show ipv6 cef exact-route** command in user EXEC or privileged EXEC mode.

show ipv6 cef exact-route *session-source-address* [**src-port** *port-number*] *session-destination-address* [**dest-port** *port-number*] [**gtp-teid** *teid*]

Syntax Description

session-source-address	The network source IPv6 address.
src-port	(Optional) Specifies a source port.
port-number	(Optional) The Layer 4 port number of the source IPv6 address, if configured. The range is from 0 to 65535.
session-destination-address	The network destination IPv6 address.
dest-port	(Optional) Specifies a destination port.
port-number	(Optional) The Layer 4 port number of the destination IPv6 address, if configured. The range is from 0 to 65535. To display the exact route for a specific GPRS Tunneling Protocol Tunnel Endpoint Identifier (GTP TEID), the *port number* for the destination port must be 2152.
gtp-teid	(Optional) Displays the exact route of a source-destination IPv6 address pair with a specific GTP TEID value.
teid	GTP TEID value. The value range is from 1 to 4294967295.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(11)T	This command was modified. The **src-port** *port-number* and **dest-port** *port-number* keywords and arguments were added.

Release	Modification
3.10S	This command is supported in Cisco IOS XE Release 3.10S. The **gtp-teid** keyword and the *teid* argument were added to the command.

Usage Guidelines

The **show ipv6 cef exact-route** command is similar to the **show ip cef exact-route** command, except that it is IPv6 specific.

The **show ipv6 cef exact-route** command displays the exact route for a source-destination IPv6 address pair.

Examples

The following is sample output from the **show ipv6 cef exact-route** command. (The fields in the display are self-explanatory)

```
Router# show ipv6 cef exact-route 77::77 10:10:10:10::11
 77::77 -> 10:10:10:10::11 : Ethernet0/0 (next hop 10:10:10:10::11)
```

Examples

The following is a sample output of the **show ipv6 cef exact-route** *session-source-address session-destination-address* [**dest-port** *port-number*] [**gtp-teid** *teid*] command. (The fields in the display are self-explanatory)

```
Router# show ipv6 cef exact-route 2011:1::1:2 2022:2::1:2 dest-port 2152 gtp-teid 100
2011:1::1:2 -> 2022:2::1:2 => IPV6 adj out of GigabitEthernet2/1/0.2, addr
FE80::21F:CAFF:FE16:3210
```

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair.
show ipv6 cef adjacency	Displays Cisco Express Forwarding for IPv6 recursive and direct prefixes resolved through an adjacency.
show ipv6 route	Displays IPv6 router advertisement information received from onlink routers.

show ipv6 cef neighbor discovery throttling

To display the Cisco Express Forwarding for IPv6 neighbor discovery (ND) throttling list, use the **show ipv6 cef neighbor discovery throttling**command in privileged EXEC mode.

show ipv6 cef neighbor discovery throttling [**internal**]

Syntax Description

internal	(Optional) Displays internal data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ipv6 cef neighbor discovery throttling** command:

```
Router# show ipv6 cef neighbor discovery throttling
Address                                   Holdtime
2001:1111::1                              00:00:02.296
```

The table below describes the fields shown in the display.

Table 38: show ipv6 cef neighbor discovery throttling Field Descriptions

Field	Description
Address	The IPv6 address for which the information on ND throttling list is displayed.
Holdtime	Length of time (in hours, minutes, and seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down.

Related Commands

Command	Description
show ipv6 neighbors	Displays IPv6 ND cache information.

show ipv6 cef non-recursive

To display nonrecursive route entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef non-recursive**command in user EXEC or privileged EXEC mode.

show ipv6 cef non-recursive [{**detail** | **internal** | **samecable**}] [**platform** [{**detail** | **internal** | **samecable**}]] [**source** [{**internal** | **epoch** *epoch-number* [{**internal** | **samecable** | **platform** [{**detail** | **internal** | **samecable**}]}]}]] [**epoch** *epoch-number* [{**internal** | **samecable** | **platform** [{**detail** | **internal** | **samecable**}]}]]

Syntax Description

detail	(Optional) Displays detailed nonrecursive route entry information.
internal	(Optional) Displays data for nonrecursive route entries.
samecable	(Optional) Displays the connected (up) interface for nonrecursive route entries.
platform	(Optional) Displays platform-specific nonrecursive route entries.
source	(Optional) Displays source-specific nonrecursive route entry information.
epoch *epoch-number*	(Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **internal**, **samecable**, **platform**, **source**, and **epoch** keywords were added, and the *epoch-number* argument was added. Next hop information was removed from the command output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef non-recursive**command is similar to the **show ip cef non-recursive**command, except that it is IPv6-specific.

The **show ipv6 cef non-recursive detail** command shows detailed FIB entry information for all nonrecursive routes.

Examples

The following is sample output from the **show ipv6 cef non-recursive detail**command:

```
Router# show ipv6 cef non-recursive detail
IPv6 CEF is enabled and running
IPv6 CEF default table
8 prefixes
2001:xx::/35
     nexthop FE80::ssss:CFF:FE3D:DCC9 Tunnel55
2001:zzz:500::/40
     nexthop FE80::nnnn:801A Tunnel32
2001:zzz::/35
     nexthop 3FFE:mmm:8023:21::2 Tunnel26
3FFE:yyy:8023:37::1/128 Receive
  Receive
3FFE:yyy:8023:37::/64 Attached, Connected
     attached to Tunnel37
3FFE:yyy:8023:38::1/128 Receive
  Receive
3FFE:yyy:8023:38::/64 Attached, Connected
     attached to Tunnel40
3FFE:yyy:8023:39::1/128 Receive
  Receive
```

The table below describes the significant fields shown in the display.

Table 39: show ipv6 cef non-recursive Field Descriptions

Field	Description
8 prefixes	Indicates the total number of IPv6 prefixes in the Cisco Express Forwarding table.
2001:xx::/35	Indicates the IPv6 prefix of the remote network.
2001:zzz:500::/40 nexthop FE80::nnnn:801A Tunnel32	Indicates that IPv6 prefix 2001:zzz:500::/40 is reachable through this next-hop address and interface.
attached to Tunnel37	Indicates that this IPv6 prefix is a connected network on Tunnel interface 37.
Receive	Indicates that this IPv6 prefix is local to the router.

This is an example of the **show ipv6 cef non-recursive**command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef non-recursive
2003:1::/64
  attached to POS6/1/0
2003:1::1/128
  receive
2003:2::/64
  attached to Loopback0
2003:2::1/128
```

Related Commands

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 forwarding FIB.
show ipv6 cef unresolved	Displays unresolved entries in the IPv6 FIB.

show ipv6 cef platform

To display platform-specific Cisco Express Forwarding data, use the **show ipv6 cef platform**command in user EXEC or privileged EXEC mode.

show ipv6 cef platform [{**detail** | **internal** | **samecable**}]

Syntax Description

detail	(Optional) Displays detailed platform-specific Cisco Express Forwarding data.
internal	(Optional) Displays internal platform-specific Cisco Express Forwarding data.
samecable	(Optional) Displays platform-specific data for the connected (up) interface.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(22)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SCE	This command was integrated into Cisco IOS Release 12.2(33)SCE.

Usage Guidelines

If none of the optional keywords is used, data for all platforms is displayed.

Examples

The following example will display all platform-specific Cisco Express Forwarding data:

```
Router# show ipv6 cef platform
```

show ipv6 cef summary

To display a summary of the entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef summary**command in user EXEC or privileged EXEC mode.

show ipv6 cef summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef summary**command is similar to the **show ip cef summary**command, except that it is IPv6-specific.

Examples

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

```
Router# show ipv6 cef summary
IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
9 prefixes
```

The table below describes the significant fields shown in the display.

Table 40: show ipv6 cef summary Field Descriptions

Field	Description
Slow processing intvl	Indicates the waiting time (in seconds) before the software attempts to resolve any unresolved routes.
unresolved prefixes	Indicates the number of unresolved routes.

Field	Description
requiring adjacency update	Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution.

This is an example of the **show ipv6 cef summary** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef summary
IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
 Table id 0, 0 resets
 Database epoch: 0 (20 entries at this epoch)
```

Related Commands

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.
show cef interface	Displays Cisco Express Forwarding-related interface information.

show ipv6 cef switching statistics

To display switching statistics in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef switching statistics**command in privileged EXEC mode.

show ipv6 cef switching statistics [**feature**]

Syntax Description

feature	(Optional) The output is ordered by feature.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If the optional feature keyword is not used, all switching statistics are displayed.

Examples

The following is sample output from the **show ipv6 cef switching statistics**command:

```
Router# show ipv6 cef switching statistics
Reason                                    Drop       Punt  Punt2Host
RP LES Packet destined for us                0     132248          0
RP LES Multicast                             0          2          0
RP LES Link-local                            0         33          0
RP LES Total                                 0     132283          0
Slot 4 Packet destined for us                0     129546          0
Slot 4 Link-local                            0         31          0
Slot 4 Total                                 0     129577          0
All    Total                                 0     261860          0
```

The table below describes the significant fields shown in the display.

Table 41: show ipv6 cef switching statistics Field Descriptions

Field	Description
Reason	Packet description.
Drop	Number of packets dropped.
Punt	Number of packets that could be switched in the normal path and were punted to the next fastest switching vector.

Field	Description
Punt2Host	Number of packets that cannot be switched in the normal path and were punted to the host.

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 route	Displays IPv6 router advertisement information received from onlink routers.

IPv6 Commands: show ipv6 cef tr to show ipv6 in

show ipv6 cef traffic prefix-length

To display Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) traffic statistics, use the **show ipv6 cef traffic prefix-length**command in user EXEC or privileged EXEC mode.

show ipv6 cef traffic prefix-length

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef traffic prefix-length**command is similar to the **show ip cef traffic prefix-length** command, except that it is IPv6-specific.

This command is used to display CEFv6 switched traffic statistics by destination prefix length. The **ipv6 cef accounting prefix-length** command must be enabled for the counters to increment.

Examples

The following is sample output from the **show ipv6 cef traffic prefix-length**command:

```
Router#
show ipv6 cef traffic prefix-length
IPv6 prefix length switching statistics:
----------------------------------------
Prefix       Number of       Number of
Length       Packets         Bytes
----------------------------------------
     0            0               0
     1           24            3840
     2            0               0
     3           14            1120
     4            0               0
     5           10            1200
.
.
.
```

```
28              0              0
29              4            512
30              0              0
31             18           2448
32              0              0
```

The table below describes the significant fields shown in the display.

Table 42: show ipv6 cef traffic prefix-length Field Descriptions

Field	Description
Prefix Length	Destination IPv6 prefix length for Cisco Express Forwarding switched traffic.
Number of Packets	Number of packets forwarded for the specified IPv6 prefix length.
Number of Bytes	Number of bytes sent for the specified IPv6 prefix length.

Related Commands

Command	Description
ipv6 cef accounting	Enables CEFv6 network accounting.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ipv6 cef tree

To display summary information on the default tree in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef tree**command in user EXEC or privileged EXEC mode.

show ipv6 cef tree [{**statistics** | **dependents** [*prefix-filter*]}]

Syntax Description

statistics	(Optional) Displays the default tree statistics.
dependents	(Optional) Displays the dependents of the selected tree with optional prefix filter.
prefix-filter	(Optional) A prefix filter on the dependents of the selected tree.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If none of the optional keywords or arguments is used, all summary information on the default tree in the IPv6 FIB is shown.

Examples

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

```
Router# show ipv6 cef tree
VRF Default tree information:
 RTRIE storing IPv6 addresses
 6 entries (6/0 fwd/non-fwd)
 Forwarding & Non-forwarding tree:
  6 inserts, 0 delete
  8 nodes using 288 bytes
```

The table below describes the significant fields shown in the display.

Table 43: show ipv6 cef tree Field Descriptions

Field	Description
RTRIE storing IPv6 addresses	Indicates the tree type as RTRIE.
6 entries (6/0 fwd/non-fwd)	Indicates total number of prefix entries as 6 forwarding and 0 nonforwarding entries.

Field	Description
Forwarding & Non-forwarding tree	Same tree is used for forwarding and nonforwarding.
6 inserts, 0 delete	Indicates that 6 entries were inserted and 0 entries were deleted from the tree.
8 nodes using 288 bytes	Indicates a total of 8 nodes using a total of 288 bytes of memory.
*calloc failures: *number* node	This line is not present in the example output. If this line is present in output, it indicates a memory allocation error at the indicated node.

Related Commands

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.

show ipv6 cef unresolved

To display unresolved entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef unresolved**command in user EXEC or privileged EXEC mode.

show ipv6 cef unresolved [{**detail** | **internal** | **samecable**}] [**platform** [{**detail** | **internal** | **samecable**}]] [**source** [{**internal** | **epoch** *epoch-number* [{**internal** | **samecable** | **platform** [{**detail** | **internal** | **samecable**}]}]}]] [**epoch** *epoch-number* [{**internal** | **samecable** | **platform** [{**detail** | **internal** | **samecable**}]}]]

Syntax Description

detail	(Optional) Displays detailed FIB entry information.
internal	(Optional) Displays data structures for unresolved routes.
samecable	(Optional) Displays the connected (up) interface for unresolved routes.
platform	(Optional) Displays platform-specific information on unresolved routes.
source	(Optional) Displays source-specific information on unresolved routes.
epoch *epoch-number*	(Optional) Displays the basic unresolved routes filtered by a specified epoch number. The epoch number range is from 0 to 255.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **internal**, **samecable**, **platform**, **source**, and **epoch** keywords were added. The *epoch-number* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show ipv6 cef unresolved**command is similar to the **show ip cef unresolved**command, except that it is IPv6-specific.

The **show ipv6 cef unresolved detail** command displays detailed information for all unresolved FIB entries.

Examples

The following is sample output from the **show ipv6 cef unresolved**command with the **detail** keyword:

```
Router# show ipv6 cef unresolved detail
IPv6 CEF is enabled for distributed  and running
VRF Default:
 5 prefixes (5/0 fwd/non-fwd)
 Table id 0, version 5, 0 resets
 Database epoch: 2 (5 entries at this epoch)
```

The table below describes the significant fields shown in the display.

Table 44: show ipv6 cef unresolved Field Descriptions

Field	Description
5 prefixes (5/0 fwd/non-fwd)	Indicates how many IPv6 prefixes are being used for forwarding or not forwarding.
Table id 0, version 5, 0 resets	Provides information about the Cisco Express Forwarding table.
Database epoch: 2 (5 entries at this epoch)	The epoch number of any unresolved database epochs.

This is an example of the **show ipv6 cef unresolved detail**command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef unresolved detail
```

No unresolved adjacencies exist, therefore nothing is displayed in the output of the **show ipv6 cef unresolved detail**command.

Related Commands

Command	Description
show cef interface	Displays Cisco Express Forwarding-related interface information.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef summary	Displays a summary of the entries in the IPv6 FIB.

show ipv6 cef vrf

To display the Cisco Express Forwarding Forwarding Information Base (FIB) associated with an IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ipv6 cef vrf**command in user EXEC or privileged EXEC mode.

show ipv6 cef vrf [{*vrf-name* | * | **internal**}]

Syntax Description

vrf-name	(Optional) Name assigned to the VRF.
*	(Optional) All VRFs are displayed.
internal	(Optional) Only internal data is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **show ipv6 cef vrf** command to display content of the IPv6 FIB for the specified VRF.

Examples

The following is sample output from a Cisco Express Forwarding FIB associated with a VRF named cisco1:

```
Router# show ipv6 cef vrf cisco1
 2001:8::/64
  attached to FastEthernet0/0
 2001:8::3/128
  receive
 2002:8::/64
  nexthop 10.1.1.2 POS4/0 label 22 19
 2010::/64
  nexthop 2001:8::1 FastEthernet0/0
 2012::/64
  attached to Loopback1
 2012::1/128
  receive
```

The table below describes the significant fields shown in the display.

Table 45: show ipv6 cef vrf Field Descriptions

Field	Description
2001:8::/64	Specifies the network prefix.
attached to FastEthernet0/0	Specifies the VRF interface.
nexthop 10.1.1.2 POS4/0 label 22 19	Specifies the BGP next hop address.

show ipv6 cef with epoch

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) information filtered for a specific epoch, use the **show ipv6 cef with epoch** command in privileged EXEC mode.

show ipv6 cef with epoch *epoch-number* [{**checksum** | **detail** | **internal** [**checksum**] | **platform** [{**checksum** | **detail** | **internal** [**checksum**]}]}]

Syntax Description

epoch-number	Number of the epoch, from 0 to 255.
checksum	(Optional) Displays FIB entry checksums.
detail	(Optional) Displays detailed information about FIB epochs.
internal	(Optional) Displays internal data structure information.
platform	(Optional) Displays platform-specific data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to display information about prefix properties for a specified epoch in the Cisco Express Forwarding IPv6 FIB. This command is similar to the **show ip cef with epoch** command, except that it is IPv6 specific. Use the **show ipv6 cef epoch**command to display entries filtered by epoch number.

Examples

The following is sample output from the **show ipv6 cef with epoch**command:

```
Router# show ipv6 cef with epoch 0
::/0
  no route
::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
```

```
2001::/64
  attached to Ethernet2/0
2001::1/128
  receive for Ethernet2/0
2001::3/128
  attached to Ethernet2/0
2001:1::/64
  attached to Ethernet0/0
2001:1::1/128
  receive for Ethernet0/0
2001:2::/64
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
  attached to Tunnel0
2002::1/128
  receive for Tunnel0
FE80::/10
  receive for Null0
FF00::/8
  receive for Null0
```

The table below describes significant fields shown in the display.

Table 46: show ipv6 cef with epoch Field Descriptions

Field	Description
no route	No route is associated with the IPv6 prefix.
discard	Traffic for this prefix is discarded.
2000::1/128 receive for Loopback0	A receive prefix for interface Loopback0.
2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0	An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0.
2001::/64 attached for Ethernet2/0	This prefix is a connected network on interface Ethernet 0/0.
2001::1/128 receive for Ethernet2/0	A receive prefix for interface Ethernet 0/0.

The following is sample output from the **show ipv6 cef with epoch detail**command:

```
Router# show ipv6 cef with epoch 0 detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)
::/0, epoch 0, flags default route handler
  no route
::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
```

```
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
  attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
```

The table below describes significant fields shown in the display.

Table 47: show ipv6 cef with epoch detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally	Indicates that IPv6 CEF is enabled and running on the RP.
VRF base 16 prefixes (16/0 fwd/non-fwd)	Number of prefixes in the VRF, how many of them are forwarded, and how many are not forwarded.
Table id 0	Table identification number.
Database epoch 0 (16 entries at this epoch)	Value of the database epoch and number of entries in the epoch.
2000::1/128, epoch 0, flags attached, connected, receive, local receive for Loopback0	Provides detail for the table entries. In this example, 2000:1/128 is an IPv6 prefix at epoch 0. The flags set for this prefix are: • attached--Prefix is a connected network • connected--Prefix includes an address that is bound to an interface on the device • receive--Prefix is punt to and handled by the process level • local--Prefix is a subset of receive and marks prefixes that are received by on interface on the device

The following is sample output from the **show ipv6 cef with epoch checksum** command:

```
Router# show ipv6 cef with epoch 0 checksum
::/0
  FIB checksum: 0x64E25610
::/127
  FIB checksum: 0xE0B3DE11
2000::1/128
  FIB checksum: 0xD04E36EC
2000::2/128
  FIB checksum: 0x84892BA5
2000::3/128
  FIB checksum: 0x912BA720
2000::4/128
  FIB checksum: 0xC6D89ADA
.
.
.
```

The table below describes significant fields shown in the display.

Table 48: show ipv6 cef with epoch checksum Field Descriptions

Field	Description
::/0	Default route handler. ::/0 prefix matches all addresses. (::/128 prefix is an exact match for all zero addresses only.)
FIB checksum: 0x64E25610	FIB checksum associated with the named prefix.

Related Commands

Command	Description
show ip cef with epoch	Displays Cisco Express Forwarding FIB information filtered for a specific epoch.
show ipv6 cef	Displays entries in the IPv6 FIB.
show ipv6 cef epoch	Displays a summary of IPv6 FIB epoch information.

show ipv6 cef with source

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) filtered for a specific source, use the **show ipv6 cef with source** command in privileged EXEC mode.

show ipv6 cef with source *source-type* [{**checksum** | **detail** | **epoch** | **internal** [**checksum**] | **platform** [{**checksum** | **detail** | **internal** [**checksum**]}]}]

Syntax Description

source-type	The *source-type*argument must be replaced by one of the following keywords that are supported for your release. Keywords for all supported Cisco IOS releases: • **alias** --Displays alias address prefix sources in the Cisco Express Forwarding IPv6 FIB. • **broadband** --Displays broadband receive prefix sources in the Cisco Express Forwarding IPv6 FIB. • **fallback** --Displays fallback lookup prefix sources in the Cisco Express Forwarding IPv6 FIB. • **interface** --Displays interface configuration prefix sources in the Cisco Express Forwarding IPv6 FIB. • **nat** --Displays Network Address Translation (NAT) prefix sources in the Cisco Express Forwarding IPv6 FIB. • **rib** --Displays Routing Information Base (RIB) prefix sources in the Cisco Express Forwarding IPv6 FIB. • **special** --Displays special prefix sources in the Cisco Express Forwarding IPv6 FIB. • **test** --Displays test command prefix sources in the Cisco Express Forwarding IPv6 FIB. • **virtual** --Displays virtual address prefix sources in the Cisco Express Forwarding IPv6 FIB, for example, Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) addresses. Additional keywords for Cisco IOS Releases 12.2(25)S, 12,2(28)SB, 12.2(33)SRA, and later SB and SR releases: • **adjacency** --Displays adjacency prefix sources in the Cisco Express ForwardingIPv6 FIB. • **default-route** --Displays default route handler prefix sources in the Cisco Express Forwarding FIB. • **inherited-path-list** --Displays inherited path list prefix source in the Cisco Express Forwarding FIB. Additional keywords for Cisco IOS Releases 12.2(33)SXH, 12.4(20)T, and later SX and T releases: • **adj** --Displays adjacency prefix sources in the Cisco Express Forwarding FIB.

-	• **defnet--** Displays default network prefix sources in the Cisco Express Forwarding IPv6 FIB. • **defroutehandler** --Displays default route handler prefix sources in the Cisco Express Forwarding IPv6 FIB. • **ipl** --Displays inherited path list prefix source in the Cisco Express ForwardingIPv6 FIB. • **recursive-resolution** --Displays recursive resolution prefix sources in the Cisco Express Forwarding IPv6 FIB. Additional keyword for Cisco IOS Release 12.2(33)SXH and later SX releases: • **lte** --Displays Multiprotocol Label Switching (MPLS) label table entries.
checksum	(Optional) Displays IPv6 FIB entry checksums.
detail	(Optional) Displays detailed information about IPv6 FIB epochs.
epoch	(Optional) Displays information about epochs associated with the source prefix.
internal	(Optional) Displays internal data structure information.
platform	(Optional) Displays platform-specific data structures.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to filter on prefixes in the Cisco Express Forwarding FIB that are added by a specified source.

Examples

Examples For All Supported Releases

The following is sample output from the **show ipv6 cef with source rib** command:

```
Router# show ipv6 cef with source rib
::/127
  discard
2000::1/128
  receive for Loopback0
```

```
2000::2/128
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
  attached to Ethernet2/0
2001::1/128
  receive for Ethernet2/0
2001:1::/64
  attached to Ethernet0/0
2001:1::1/128
  receive for Ethernet0/0
2001:2::/64
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
  attached to Tunnel0
2002::1/128
  receive for Tunnel0
FE80::/10
  receive for Null0
FF00::/8
  receive for Null0
```

The table below describes the significant fields shown in the display.

Table 49: show ipv6 cef with source rib Field Descriptions

Field	Description
::/127	IPv6 prefix.
discard	Indicates that traffic destined for this prefix should be discarded.
2000::1/128 receive for Loopback0	An IPv6 prefix that is a receive prefix for interface Loopback0. Traffic destined for this prefix will be punted to the process level.
2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0	An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0.
2001::/64 attached for Ethernet2/0	An IPv6 prefix that is a connected network on interface Ethernet 0/0. That is, the destination can be reached directly through the specified interface.

The following is sample output from the **show ipv6 cef with source fib detail** command:

```
Router# show ipv6 cef with source rib detail
IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)
::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
```

```
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
  attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
```

The table below describes the significant fields shown in the display.

Table 50: show ipv6 cef with source rib detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled globally.
VRF base	Base VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many prefixes are forwarded, and how many are not forwarded.
Table id 0	Identifies the table by number.
Database epoch:	Specifies the type of epoch.
0 (16 entries at this epoch)	Number of the epoch (0) and number of entries in the epoch.
2000::1/128, epoch 0, flags attached, connected, receive, local	Details about the prefix: the epoch in which it is found, the flags set for the prefix: • attached--Prefix is a connected network • connected--Prefix includes an address that is bound to an interface on the device • receive--Prefix is punt to and handled by the process level • local--Prefix is a subset of receive and marks prefixes that are received by on interface on the device

Examples for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and Later SB and SR Releases

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

```
Router# show ipv6 cef with source adjacency
2001::3/128
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 51: show ipv6 cef with source adjacency Field Descriptions

Field	Description
20001::3/128	IPv6 prefix whose source is an adjacency.
attached to Ethernet2/0	Indicates that the prefix is a connected network through Interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adjacency detail**command:

```
Router# show ipv6 cef with source adjacency detail
#
IPv6 CEF is enabled and running centrally.
VRF Default
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0x1E000000
 Database epoch:        0 (16 entries at this epoch)
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 050878F0
   Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 52: show ipv6 cef with source adjacency detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled and running on the RP.
VRF Default	Default VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes in the VRF, how many prefixes are forwarded and how many are not forwarded.
Table id 0x1E000000	Identifies the table by hexadecimal number.
2001::3/128, epoch 0, flags attached	Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network.
Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0	Indicates that the prefix was sourced by an adjacency and specifies the address family, interface, and address in memory of the adjacency.

Field	Description
Dependent covered prefix type adjfib cover 2001::/64	A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed.
attached to Ethernet2/0	Indicates the prefix is a connect network through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adjacency checksum**command:

```
Router# show ipv6 cef with source adjacency checksum
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

The table below describes the significant fields shown in the display.

Table 53: show ipv6 cef with source adjacency checksum Field Descriptions

Field	Description
2001::3/128	IPv6 prefix whose source is an adjacency.
FIB checksum: 0x4AE0F5DC	FIB checksum.

Examples for Cisco IOS Releases 12.2(33)SXH, 12.4(20)T and Later SX and T Releases

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

```
Router# show ipv6 cef with source adj
2001::3/128
  attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 54: show ipv6 cef with source adj Field Descriptions

Field	Description
20001::3/128	IPv6 prefix whose source is an adjacency.
attached to Ethernet2/0	Indicates that the prefix is a network connected through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adj detail**command:

```
Router# show ipv6 cef with source adj detail
IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
 Table id 0
 Database epoch:        0 (16 entries at this epoch)
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
```

```
 Dependent covered prefix type adjfib cover 2001::/64
attached to Ethernet2/0
```

The table below describes the significant fields shown in the display.

Table 55: show ipv6 cef with source adj detail Field Descriptions

Field	Description
IPv6 CEF is enabled and running centrally.	Verifies that Cisco Express Forwarding for IPV6 is enabled an running on the RP.
VRF base	Base VRF table.
16 prefixes (16/0 Fwd/non-fwd)	Number of prefixes, and how many prefixes are forwarded and how many are not forwarded.
2001::3/128, epoch 0, flags attached	Provides more detail about the adjacency source, such as epoch number and flags.
Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0	Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network.
Dependent covered prefix type adjfib cover 2001::/64	A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed.
attached to Ethernet2/0	Indicates the prefix is a connect network through interface Ethernet 2/0.

The following is sample output from the **show ipv6 cef with source adj checksum**command:

```
Router# show ipv6 cef with source adj checksum
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

The table below describes the significant fields shown in the display.

Table 56: show ipv6 cef with source adj checksum Field Descriptions

Field	Description
2001::3/128	IPv6 prefix whose source is an adjacency.
FIB checksum: 0x4AE0F5DC	FIB checksum.

Related Commands

Command	Description
show ip cef	Displays entries in the FIB or displays a summary of the FIB.
show ip cef with epoch	Displays information about an epoch in the Cisco Express Forwarding FIB.
show ipv6 cef with epoch	Displays information about an epoch in the Cisco Express Forwarding IPv6 FIB.

Command	Description
show ipv6 cef with source	Displays information about prefix sources in the Cisco Express Forwarding IPv6 FIB.

show ipv6 cga address-db

To display IPv6 cryptographically generated addresses (CGA) from the address database, use the **show ipv6 cga address-db** command in privileged EXEC mode.

show ipv6 cga address-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGAs are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays CGAs in the CGA database:

```
Router# show ipv6 cga address-db
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
FE80::/64 ::3824:3CE4:C044:8D65 - table 0x12000003
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
```

The table below describes the significant fields shown in the display.

Table 57: show ipv6 cga address-db Field Descriptions

Field	Description
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0	CGA address for which information is shown.
interface:	Interface on which the address is configured.
modifier:	The CGA modifier.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 cga modifier-db

To display IPv6 cryptographically generated address (CGA) modifier database entries, use the **show ipv6 cga modifier-db** command in privileged EXEC mode.

show ipv6 cga modifier-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGA modifiers are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 cga modifier-db** command is used to display the modifiers generated with the **ipv6 cga modifier** command and the addresses generated from them.

Examples

The following example displays CGA modifiers in the CGA modifier database:

```
Router# show ipv6 cga modifier-db
F046:E042:13E8:1661:96E5:DD05:94A8:FADC
        label:          SubCA11
        sec level:      1
        Addresses:
  2001:100::38C9:4A1A:2972:794E
  FE80::289C:3308:4719:87F2
```

The table below describes the significant fields shown in the display.

.

Table 58: show ipv6 cga modifier-db Field Descriptions

Field	Description
D695:5D75:F9B5:9715:DF0A:D840:70A2:84B8	The CGA modifier for which the information is displayed.
label	Name used for the Rivest, Shamir, and Adelman (RSA) key pair.
Addresses: 2001:100::38C9:4A1A:2972:794EFE80::289C:3308:4719:87F2	The CGA address.

Related Commands

Command	Description
ipv6 cga modifier	Generates an IPv6 CGA modifier for a specified RSA key pair.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 destination-guard policy

To display destination guard information, use the **show ipv6 destination-guard policy** command in privileged EXEC mode.

show ipv6 destination-guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of the destination guard policy.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

If the *policy-name* argument is specified, only the specified policy information is displayed. If the *policy-name* argument is not specified, information is displayed for all policies.

Examples

The following is sample output from the **show ipv6 destination-guard policy** command when the policy is applied to a VLAN:

```
Device# show ipv6 destination-guard policy pol1
Destination guard policy destination:
  enforcement always
        Target: vlan 300
```

Related Commands

Command	Description
ipv6 destination-guard policy	Defines the destination guard policy.

show ipv6 dhcp

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **show ipv6 dhcp** command uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples

The following is sample output from the **show ipv6 dhcp**command. The output is self-explanatory:

```
Router# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4	This command was modified. Command output was updated to display a PPP username associated with a binding.
12.4(24)T	This command was modified. Command output was updated to display address bindings.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name*keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# show ipv6 dhcp binding
Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
            preferred lifetime 150, valid lifetime 300
```

```
            expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:58 PM (288 seconds)
```

The table below describes the significant fields shown in the display.

Table 59: show ipv6 dhcp binding Field Descriptions

Field	Description
Client	Address of a specified client.
DUID	DHCP unique identifier (DUID).
Virtual-Access2.1	First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.
Username : client_1	The username associated with the binding.
IA PD	Collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime settings, in seconds, for the specified client.
Expires at	Date and time at which the valid lifetime expires.
Virtual-Access2.2	Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username is associated with the binding is displayed in output from the **show ipv6 dhcp binding** command. If there is no PPP username associated with the binding, this field value is displayed as "unassigned."

The following example shows that the PPP username associated with the binding is "client_1":

```
Router# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : client_1
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 75, T2 135
    Prefix: 2001:0DB8:1:3::/80
```

```
            preferred lifetime 150, valid lifetime 300
            expires at Aug 07 2008 05:19 AM (225 seconds)
```

The following example shows that the PPP username associated with the binding is unassigned:

```
Router# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : unassigned
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 150, T2 240
    Prefix: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 binding table.

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp database [*agent-URL*]

Syntax Description

agent-URL	(Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the **ipv6 dhcp database** command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The **show ipv6 dhcp database**command displays DHCP for IPv6 binding database agent information. If the *agent-URL* argument is specified, only the specified agent is displayed. If the *agent-URL* argument is not specified, all database agents are shown.

Examples

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

```
Router# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
```

```
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614
```

The table below describes the significant fields shown in the display.

Table 60: show ipv6 dhcp database Field Descriptions

Field	Description
Database agent	Specifies the database agent.
Write delay	The amount of time (in seconds) to wait before updating the database.
transfer timeout	Specifies how long (in seconds) the DHCP server should wait before terminating a database transfer. Transfers that exceed the timeout period are terminated.
Last written	The last date and time bindings were written to the file server.
Write timer expires...	The length of time, in seconds, before the write timer expires.
Last read	The last date and time bindings were read from the file server.
Successful/failed read times	The number of successful or failed read times.
Successful/failed write times	The number of successful or failed write times.

Related Commands

Command	Description
ipv6 dhcp database	Specifies DHCP for IPv6 binding database agent parameters.

show ipv6 dhcp guard policy

To display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard information, use the **show ipv6 dhcp guard policy** command in privileged EXEC mode.

show ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

If the *policy-name* argument is specified, only the specified policy information is displayed. If the *policy-name* argument is not specified, information is displayed for all policies.

Examples

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

```
Router#show ipv6 dhcp guard policy

Dhcp guard policy: default
        Device Role: dhcp client
        Target: Et0/3

Dhcp guard policy: test1
        Device Role: dhcp server
        Target: vlan 0    vlan 1    vlan 2    vlan 3    vlan 4
        Max Preference: 200
        Min Preference: 0
        Source Address Match Access List: acl1
        Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
        Device Role: dhcp relay
        Target: Et0/0 Et0/1 Et0/2
```

The table below describes the significant fields shown in the display.

Table 61: show ipv6 dhcp guard Field Descriptions

Field	Description
Device Role	The role of the device. The role is either client, server or relay.

Field	Description
Target	The name of the target. The target is either an interface or a VLAN.

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp interface [*type number*]

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(11)T	Command output was modified to allow relay agent information to be displayed on a specified interface if the relay agent feature is configured on that interface.
12.4(24)T	Command output was updated to display interface address assignments and T1 and T2 renew/rebind times.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Examples

The following is sample output from the **show ipv6 dhcp interface**command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Router1# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
```

```
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
                expires at Nov 08 2002 09:10 AM (54319 seconds)
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
                expires at Nov 08 2002 09:11 AM (54331 seconds)
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
                expires at Nov 08 2002 08:17 AM (51109 seconds)
      DNS server: 1001::1
      DNS server: 1001::2
      Domain name: domain1.net
      Domain name: domain2.net
      Domain name: domain3.net
    Prefix name is cli-p1
    Rapid-Commit is enabled
```

The table below describes the significant fields shown in the display.

Table 62: show ipv6 dhcp interface Field Descriptions

Field	Description
Ethernet2/1 is in server/client mode	Displays whether the specified interface is in server or client mode.
Preference value:	The advertised (or default of 0) preference value for the indicated server.
Prefix name is cli-p1	Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored.
Using pool: svr-p1	The name of the pool that is being used by the interface.
State is OPEN	State of the DHCP for IPv6 client on this interface. "Open" indicates that configuration information has been received.
List of known servers	Lists the servers on the interface.
Address, DUID	Address and DHCP unique identifier (DUID) of a server heard on the specified interface.
Rapid commit is disabled	Displays whether the **rapid-commit** keyword has been enabled on the interface.

The following example shows the DHCP for IPv6 relay agent configuration on FastEthernet interface 0/0, and use of the **show ipv6 dhcp interface** command displays relay agent information on FastEthernet interface 0/0:

```
Router(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
Router# show ipv6 dhcp interface FastEthernet 0/0
FastEthernet0/0 is in relay mode
  Relay destinations:
    FE80::250:A2FF:FEBF:A056 via FastEthernet0/1
```

Related Commands

Command	Description
ipv6 dhcp client pd	Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface.

Command	Description
ipv6 dhcp relay destination	Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp pool [*poolname*]

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	Command output was updated to display address pools and prefix pools.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **ipv6 dhcp pool** command to create a configuration pool, and use the **ipv6 dhcp server** command to associate the configuration pool with a server on an interface.

The **show ipv6 dhcp pool** command displays DHCP for IPv6 configuration pool information. If the *poolname* argument is specified, only information on the specified pool is displayed. If the *poolname* argument is not specified, information about all pools is shown.

Examples

The following sample output displays DHCP for IPv6 configuration pool information:

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
```

```
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: example1.net
  Domain name: example2.net
  Domain name: example3.net
Active clients: 2
```

The table below describes the significant fields shown in the display.

Table 63: show ipv6 dhcp pool Field Descriptions

Field	Description
DHCPv6 pool: svr-p1	The name of the pool.
IA PD	Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes to be delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	Lifetimes, in seconds, associated with the prefix statically assigned to the specified client.
DNS server	IPv6 addresses of the DNS servers.
Domain name	Displays the DNS domain search list.
Active clients	Total number of active clients.

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.

show ipv6 dhcp relay binding

To display DHCPv6 Internet Assigned Numbers Authority (IANA) and DHCPv6 Identity Association for Prefix Delegation (IAPD) bindings on a relay agent, use the **show ipv6 dhcp relay binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp relay binding [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)S	This command was modified. In addition to DHCPv6 IAPD bindings, DHCPv6 IANA bindings on a relay agent can be displayed.
Cisco IOS XE Release 3.5S	This command was modified. In addition to DHCPv6 IAPD bindings, DHCPv6 IANA bindings on a relay agent can be displayed.
12.2(33)SCF4	This command was implemented on Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

If the **vrf** *vrf-name* keyword-argument pair is specified, all bindings belonging to the specified VRF are displayed.

Note Only the DHCPv6 IAPD bindings on a relay agent are displayed on the Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.

Examples

The following is sample output from the **show ipv6 dhcp relay binding** command:

```
Device# show ipv6 dhcp relay binding
```

The following example shows output from the **show ipv6 dhcp relay binding** command with a specified VRF name on a Cisco uBR10012 universal broadband device:

```
Device# show ipv6 dhcp relay binding vrf vrf1

Prefix: 2001:DB8:0:1:/64 (Bundle100.600)
  DUID: 000300010023BED94D31
```

```
IAID: 3201912114
lifetime: 600
```

The table below describes the significant fields shown in the display.

Table 64: show ipv6 dhcp relay binding Field Descriptions

Field	Description
Prefix	IPv6 prefix for DHCP.
DUID	DHCP Unique Identifier (DUID) for the IPv6 relay binding.
IAID	Identity Association Identification (IAID) for DHCP.
lifetime	Lifetime of the prefix, in seconds.

Related Commands

Command	Description
clear ipv6 dhcp relay binding	Clears a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding.

show ipv6 eigrp events

To display Enhanced Interior Gateway Routing Protocol (EIGRP) events logged for IPv6, use the **show ipv6 eigrp events** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp events [{[{**errmsg** | **sia**}] [*event-num-start event-num-end*] | **type**}]

Syntax Description

errmsg	(Optional) Displays error messages being logged.
sia	(Optional) Displays Stuck In Active (SIA) messages.
event-num-start	(Optional) Starting number of the event range. The range is from 1 to 4294967295.
event-num-end	(Optional) Ending number of the event range. The range is from 1 to 4294967295.
type	(Optional) Displays event types being logged.

Command Default

If no event range is specified, information for all IPv6 EIGRP events is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1) on the Cisco 3845 series routers.

Usage Guidelines

The **show ipv6 eigrp events**command is used to analyze a network failure by the Cisco support team and is not intended for general use. This command provides internal state information about EIGRP and how it processes route notifications and changes.

Examples

The following is sample output from the **show ipv6 eigrp events** command. The fields are self-explanatory.

```
Router# show ipv6 eigrp events
Event information for AS 65535:
1    00:56:41.719 State change: Successor Origin Local origin
2    00:56:41.719 Metric set: 2555:5555::/32 4294967295
3    00:56:41.719 Poison squashed: 2555:5555::/32 lost if
4    00:56:41.719 Poison squashed: 2555:5555::/32 rt gone
5    00:56:41.719 Route installing: 2555:5555::/32 FE80::ABCD:4:EF00:1
6    00:56:41.719 RDB delete: 2555:5555::/32 FE80::ABCD:4:EF00:2
7    00:56:41.719 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:1
8    00:56:41.719 Find FS: 2555:5555::/32 4294967295
9    00:56:41.719 Free reply status: 2555:5555::/32
10   00:56:41.719 Clr handle num/bits: 0 0x0
11   00:56:41.719 Clr handle dest/cnt: 2555:5555::/32 0
12   00:56:41.719 Rcv reply met/succ met: 4294967295 4294967295
13   00:56:41.719 Rcv reply dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
14   00:56:41.687 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:2
15   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
```

```
16   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
17   00:56:41.687 State change: Local origin Successor Origin
18   00:56:41.687 Metric set: 2555:5555::/32 4294967295
19   00:56:41.687 Active net/peers: 2555:5555::/32 65536
20   00:56:41.687 FC not sat Dmin/met: 4294967295 2588160
21   00:56:41.687 Find FS: 2555:5555::/32 2588160
22   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
23   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:1
24   00:56:41.659 Change queue emptied, entries: 1
25   00:56:41.659 Metric set: 2555:5555::/32 2588160
```

Related Commands

Command	Description
clear ipv6 eigrp	Deletes entries from EIGRP for IPv6 routing tables.
debug ipv6 eigrp	Displays information about EIGRP for IPv6 protocol.
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.

show ipv6 eigrp interfaces

To display information about interfaces configured for the Enhanced Interior Gateway Routing Protocol (EIGRP) in IPv6 topologies, use the **show ipv6 eigrp interfaces** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp [*as-number*] **interfaces** [*type number*] [**detail**]

Syntax Description

as-number	(Optional) Autonomous system number.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed interface information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. Information about the Equal Cost Multipath (ECMP) mode was included in the command output.
Cisco IOS XE Release 3.5S	This command was modified. Information about the ECMP mode was included in the command output.
15.2(3)T	This command was modified. Information about the ECMP mode was included in the command output.

Usage Guidelines

Use the **show ipv6 eigrp interfaces** command to determine the interfaces on which EIGRP is active and to get information about EIGRP processes related to those interfaces. The optional *type number* argument and the **detail** keyword can be entered in any order.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

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

```
Device# show ipv6 eigrp 1 interfaces

IPv6-EIGRP interfaces for process 1
                     Xmit Queue    Mean    Pacing Time    Multicast     Pending
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0         0         0/0           0        0/10           0           0
```

The following is sample output from the **show ipv6 eigrp interfaces detail** command:

```
Device# show ipv6 eigrp interfaces detail

IPv6-EIGRP interfaces for process 1
                     Xmit Queue    Mean    Pacing Time    Multicast    Pending
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0          0       0/0            0        0/10           0            0
Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set
```

The following sample output from the **show ipv6 eigrp interface detail** command displays detailed information about a specific interface on which the **no ipv6 next-hop self** command is configured with the **no-ecmp-mode** option:

```
Device# show ipv6 eigrp interfaces detail tunnel 0

EIGRP-IPv6 Interfaces for AS(1)
                        Xmit Queue   PeerQ        Mean   Pacing Time   Multicast   Pending

Interface        Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Tu0/0              2        0/0       0/0          29       0/0         136           0
Hello-interval is 5, Hold-time is 15
  Split-horizon is disabled
  Next xmit serial <none>
  Packetized sent/expedited: 48/1
  Hello's sent/expedited: 13119/49
  Un/reliable mcasts: 0/20  Un/reliable ucasts: 31/398
  Mcast exceptions: 5  CR packets: 5  ACKs suppressed: 1
  Retransmissions sent: 355  Out-of-sequence rcvd: 6
  Next-hop-self disabled, next-hop info forwarded, ECMP mode Enabled
  Topology-ids on interface - 0
  Authentication mode is not set
```

The table below describes the significant fields shown in the displays.

Table 65: show ipv6 eigrp interfaces Field Descriptions

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.

Field	Description
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time (SRTT) interval (in seconds).
Pacing Time Un/Reliable	Pacing time (in seconds) used to determine when EIGRP packets (unreliable and reliable) should be sent out of the interface.
Multicast Flow Timer	Maximum number of seconds in which the device will send multicast EIGRP packets.
Pending Routes	Number of routes in the transmit queue waiting to be sent.
Hello interval is 5 sec	Length (in seconds) of the hello interval.

show ipv6 eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp neighbors [{*interface-typeas-number* | **static** | **detail**}]

Syntax Description

interface-type	(Optional) Interface type.
as-number	(Optional) Autonomous system number.
static	(Optional) Displays static routes.
detail	(Optional) Displays detailed neighbor information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **show ipv6 eigrp neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

Examples

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

```
Router# show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H Address                      Interface      Hold      Uptime     SRTT     RTO   Q     Seq
                                              (sec)                (ms)           Cnt   Num
0 Link-local address:             Et0/0         14        00:00:13   11      200   0      2
FE80::A8BB:CCFF:FE00:200
```

The table below describes the significant fields shown in the display.

Table 66: show ipv6 eigrp neighbors Field Descriptions

Field	Description
process 1	Autonomous system number.
Address FE80::A8BB:CCFF:FE00:200	IPv6 address of the EIGRP peer.

Field	Description
Interface	Interface on which the router is receiving hello packets from the peer.
Hold	Length of time (in seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, the nondefault hold time will be displayed.
Uptime	Elapsed time (in hours:minutes:seconds) since the local router first heard from this neighbor.
SRTT (ms)	Smoothed round-trip time (SRTT). The number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.
Q count	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.

The following is sample output from the **show ipv6 eigrp neighbors**command with the **detail** keyword:

```
Router# show ipv6 eigrp neighbors detail
IPv6-EIGRP neighbors for process 1
H  Address                   Interface      Hold      Uptime    SRTT    RTO   Q    Seq
                                           (sec)               (ms)          Cnt  Num
0  Link-local address:         Et0/0        11        00:00:30   11     200   0    2
FE80::A8BB:CCFF:FE00:200
Version 12.4/1.2, Retrans: 0, Retries: 0
```

The table below describes the significant fields shown in the display.

Table 67: show ipv6 eigrp neighbors detail Field Descriptions

Field	Description
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.
Retries	The number of times an attempt was made to retransmit a packet.

The following is sample output from the **show ipv6 eigrp neighbors**command with the **static**keyword:

```
Router# show ipv6 eigrp neighbors static
```

```
IPv6-EIGRP neighbors for process 1
Static Address Interface
Link-local address: Ethernet0/0
FE80::A8BB:CCFF:FE00:200
```

show ipv6 eigrp topology

To display Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 topology table entries, use the **show ipv6 eigrp topology** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp topology [{*as-number ipv6-address*}] [{**active** | **all-links** | **pending** | **summary** | **zero-successors**}]

Syntax Description

as-number	(Optional) Autonomous system number.
ipv6-address	(Optional) IPv6 address.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table (including nonfeasible-successor sources).
pending	(Optional) Displays all entries in the EIGRP topology table that are either waiting for an update from a neighbor or waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays the available routes that have zero successors.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. Information about the Equal Cost Multipath (ECMP) mode was included in the command output.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(2)S	This command was modified. The output of the command was enhanced to display route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The output of the command was enhanced to display route tag values in dotted-decimal format.
15.2(3)T	This command was modified. Information about the Equal Cost Multipath (ECMP) mode was included in the command output.

Usage Guidelines

If this command is used without any keywords or arguments, only routes that are feasible successors are displayed. The **show ipv6 eigrp topology** command can be used to determine Diffusing Update Algorithm (DUAL) states and to debug possible DUAL problems.

Examples

The following is sample output from the **show ipv6 eigrp topology** command. The fields in the display are self-explanatory.

```
Device# show ipv6 eigrp topology

IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

The following sample output from the **show ipv6 eigrp topology** *prefix* command displays ECMP mode information when the **no ipv6 next-hop-self** command is configured without the **no-ecmp-mode** option in the EIGRP topology. The ECMP mode provides information about the path that is being advertised. If there is more than one successor, the top most path will be advertised as the default path over all interfaces, and the message “ECMP Mode: Advertise by default” will be displayed in the output. If any path other than the default path is advertised, the message “ECMP Mode: Advertise out <Interface name>” will be displayed. The fields in the display are self-explanatory.

```
Device# show ipv6 eigrp topology 2001:DB8:10::1/128

EIGRP-IPv6 Topology Entry for AS(1)/ID(192.0.2.100) for 2001:DB8:10::1/128
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
  Descriptor Blocks:
  FE80::A8BB:CCFF:FE01:2E01 (Tunnel0), from FE80::A8BB:CCFF:FE01:2E01, Send flag is 0x0
      Composite metric is (284160/281600), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 1100 microseconds
        Reliability is 255/255
        Load is ½55
        Minimum MTU is 1400
        Hop count is 1
        Originating router is 10.10.1.1
      ECMP Mode: Advertise by default
FE80::A8BB:CCFF:FE01:3E01 (Tunnel1), from FE80::A8BB:CCFF:FE01:3E01, Send flag is 0x0
      Composite metric is (284160/281600), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 1100 microseconds
        Reliability is 255/255
        Load is ½55
        Minimum MTU is 1400
        Hop count is 1
        Originating router is 10.10.2.2
      ECMP Mode: Advertise out Tunnel1
```

Related Commands

Command	Description
show eigrp address-family topology	Displays entries in the EIGRP topology table.

show ipv6 eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets sent and received, use the **show ipv6 eigrp traffic** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp traffic [*as-number*]

Syntax Description

as-number	(Optional) Autonomous system number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **show ipv6 eigrp traffic**command to provide information on packets received and sent.

Examples

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

```
Router# show ipv6 eigrp traffic
IPv6-EIGRP Traffic Statistics for process 9
 Hellos sent/received: 218/205
 Updates sent/received: 7/23
 Queries sent/received: 2/0
 Replies sent/received: 0/2
 Acks sent/received: 21/14
```

The table below describes the significant fields shown in the display.

Table 68: show ipv6 eigrp traffic Field Descriptions

Field	Description
process 9	Autonomous system number specified in the **ipv6 router eigrp**command.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

Related Commands

Command	Description
ipv6 router eigrp	Configures the EIGRP for IPv6 routing process.

show ipv6 flow cache aggregation

To display the aggregation cache configuration, use the show ipv6 cache flow aggregation command in privileged EXEC mode.

show ipv6 flow cache aggregation aggregation-type [**verbose**]

Syntax Description

aggregation-type	Displays the configuration of a particular aggregation cache as follows: • Autonomous system • Destination prefix • Prefix • Protocol-port • Source prefix
verbose	(Optional) Displays additional information from the aggregation cache.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is an example display of an autonomous system aggregation cache using the show iv6 flow cache aggregation as command:

```
Router# show ipv6 flow cache aggregation as
IPv6 Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures
Src If       Src AS  Dst If       Dst AS  Flows   Pkts  B/Pk  Active
Fa1/0         0      Null          0         1      2     49    10.2
Fa1/0         0      Se2/0         20        1      5    100     0.0
```

The following is a sample display of an autonomous system aggregation cache for the prefix mask 2001::FFFC/64 using the show ipv6 flow cache aggregation as command:

```
Router# show ipv6 flow cache aggregation as
IPv6 Flow Switching Cache, 278544 bytes
```

```
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures
Src If         Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2             0     Null             0           1     2       49    10.2
e1/2             0     e1/2            20           1     5      100     0.0
```

The following is a sample display of an autonomous system aggregation cache for Ethernet1/2 using the show ipv6 flow cache verbose aggregation as command:

```
Router# show ipv6 flow cache aggregation as verbose
IPv6 Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures
Src If         Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2             0     Null             0           1     2       49    10.2
e1/2             0     e1/2            20           1     5      100     0.0
```

The table below describes the significant fields shown in these examples.

Table 69: show ipv6 flow cache aggregation Field Descriptions

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache, but are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
Src If	Specifies the source interface.
Src AS	Specifies the source autonomous system.
Dst If	Specifies the destination interface.
Dst AS	Specifies the destination autonomous system.
Flows	Number of flows.
Pkts	Number of packets.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	Number of active flows in the NetFlow cache at the time this command was entered.

Related Commands

Command	Description
ipv6 flow-aggregation cache	Enables aggregation cache configuration mode.

show ipv6 flow export

To display the statistics for the data export, including the main cache and all other enabled caches, use the showipv6 flow export command in user EXEC or privileged EXEC mode.

show ipv6 flow export [**template**]

Syntax Description

template	(Optional) Displays export template statistics.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

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

```
Router# show ipv6 flow export
Flow export is enabled
   Exporting flows to 10.42.42.1 (9991) 10.0.101.254 (9991)
   Exporting using source IP address 10.0.101.203
   Version 5 flow records
   Export Stats for 10.42.42.1 (9991)
           3 flows exported in 3 udp datagrams
           0 flows failed due to lack of export packet
           3 export packets were sent up to process level
           0 export packets were dropped due to no fib
           0 export packets were dropped due to adjacency issues
           0 export packets were dropped enqueuing for the RP
           0 export packets were dropped due to IPC rate limiting
   Export Stats for 10.0.101.254 (9991)
           7 flows exported in 7 udp datagrams
           0 flows failed due to lack of export packet
           6 export packets were sent up to process level
           0 export packets were dropped due to no fib
           0 export packets were dropped due to adjacency issues
           0 export packets were dropped enqueuing for the RP
           0 export packets were dropped due to IPC rate limiting
```

The table below describes the significant fields shown in the display.

Table 70: show ipv6 flow export Field Descriptions

Field	Description
Exporting flows to 10.42.42.1 (9991) 10.0.101.254 (9991)	Specifies the export destinations and ports. The ports are in parentheses.
Exporting using source IP address 10.0.101.203	Specifies the source address or interface.
Version 5 flow records	Specifies the version of the flow.
3 flows exported in 3udp datagrams	The total number of export packets sent, and the total number of flows contained within them.
0 flows failed due to lack of export packet	No memory was available to create an export packet.
0 export packets were sent up to process level	The packet could not be processed by CEF or by fast switching, possibly because another feature requires running on the packet.
0 export packets were dropped due to no fib 0 export packets were dropped due to adjacency issues	Indicates that CEF was unable to switch the packet or forward it up to the process level.
0 export packets were dropped enqueuing for the RP 0 export packets were dropped due to IPC rate limiting	Indicates that there was a problem transferring the export packet between the RP and the line card.

show ipv6 general-prefix

To display information on IPv6 general prefixes, use the **show ipv6 general-prefix** command in user EXEC or privileged EXEC mode.

show ipv6 general-prefix

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **show ipv6 general-prefix** command to view information on IPv6 general prefixes.

Examples

The following example shows an IPv6 general prefix called my-prefix, which has been defined based on a 6to4 interface. The general prefix is also being used to define an address on interface loopback42.

```
Router# show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
```

The table below describes the significant fields shown in the display.

Table 71: show ipv6 general-prefix Field Descriptions

Field	Description
IPv6 Prefix	User-defined name of the IPv6 general prefix.
Acquired via	The general prefix has been defined based on a 6to4 interface. A general prefix can also be defined manually or acquired using DHCP for IPv6 prefix delegation.
2002:B0B:B0B::/48	The prefix value for this general prefix.
Loopback42 (Address command)	List of interfaces where this general prefix is used.

Related Commands

Command	Description
ipv6 general-prefix	Defines a general prefix for an IPv6 address manually.

show ipv6 inspect

To view Context-based Access Control (CBAC) configuration and session information, use the show ipv6 inspect command in privileged EXEC mode.

show ipv6 inspect {**name inspection-name** | **config** | **interfaces** | **session** [**detail**] | **all**}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name inspection-name.
config	Displays the complete Cisco IOS firewall inspection configuration.
interfaces	Displays interface configuration with respect to applied inspection rules and access lists.
session [**detail**	Displays existing sessions that are currently being tracked and inspected by Cisco IOS firewall. The optional detail keyword causes additional details about these sessions to be shown.
all	Displays all Cisco IOS firewall configuration and all existing sessions that are currently being tracked and inspected by Cisco IOS firewall.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example asks for information about interfaces currently under inspection:

```
Router# show ipv6 inspect
 interfaces
```

Related Commands

Command	Description
ipv6 inspect	Applies a set of inspection rules to an interface.

show ipv6 interface

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

show ipv6 interface [**brief**] [*type number*] [**prefix**]

Syntax Description

brief	(Optional) Displays a brief summary of IPv6 status and configuration for each interface.
type	(Optional) The interface type about which to display information.
number	(Optional) The interface number about which to display information.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool.

Command Default

All IPv6 interfaces are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The OK, TENTATIVE, DUPLICATE, ICMP redirects, and ND DAD fields were added to the command output.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	Command output was updated to display information on the current Unicast RPF configuration.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by a device through an interface.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	Command output was updated to show Hot Standby Router Protocol (HSRP) for IPv6 information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
12.4(24)T	Command output was updated to show the Dynamic Host Configuration Protocol (DHCP) originated addresses.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

Use the **show ipv6 interface** command to validate the IPv6 status of an interface and its configured addresses. The show ipv6 interface command also displays the parameters that IPv6 is using for operation on this interface and any configured features.

If the interface's hardware is usable, the interface is marked up. If the interface can provide two-way communication for IPv6, the line protocol is marked up.

If you specify an optional interface type and number, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

Examples

Interface Information for a Specific Interface with IPv6 Configured

The **show ipv6 interface**command displays information about the specified interface.

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
  No Virtual link-local address(es):
  Global unicast address(es):
    2001::1, subnet is 2001::/64 [DUP]
    2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
    2001:100::1, subnet is 2001:100::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:6700
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
```

```
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The table below describes the significant fields shown in the display.

Table 72: show ipv6 interface Field Descriptions

Field	Description
Ethernet0/0 is up, line protocol is up	Indicates whether the interface hardware is 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, down (down is not shown in sample output)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful or IPv6 CP has been negotiated). 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.
Global unicast address(es):	Displays the global unicast addresses assigned to the interface.
Joined group address(es):	Indicates the multicast groups to which this interface belongs.
MTU	Maximum transmission unit of the interface.
ICMP error messages	Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
ICMP redirects	The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	The 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.
ND advertised reachable time	Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
ND advertised retransmit interval	Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
ND router advertisements	Specifies the interval (in seconds) for neighbor discovery router advertisements (RAs) sent on this interface and the amount of time before the advertisements expire. As of Cisco IOS Release 12.4(2)T, this field displays the default router preference (DRP) value sent by this device on this interface.
ND advertised default router preference is Medium	The DRP for the device on a specific interface.

The **show ipv6 interface** command displays information about attributes that may be associated with an IPv6 address assigned to the interface.

Attribute	Description
ANY	Anycast. The address is an anycast address, as specified when configured using the **ipv6 address** command.
CAL	Calendar. The address is timed and has valid and preferred lifetimes.
DEP	Deprecated. The timed address is deprecated.
DUP	Duplicate. The address is a duplicate, as determined by duplicate address detection (DAD). To re-attampt DAD, the user must use the **shutdown** or **no shutdown** command on the interface.
EUI	EUI-64 based. The address was generated using EUI-64.
OFF	Offlink. The address is offlink.
OOD	Overly optimistic DAD. DAD will not be performed for this address. This attribute applies to virtual addresses.
PRE	Preferred. The timed address is preferred.
TEN	Tentative. The address is in a tentative state per DAD.

Attribute	Description
UNA	Unactivated. The virtual address is not active and is in a standby state.
VIRT	Virtual. The address is virtual and is managed by HSRP, VRRP, or GLBP.

show ipv6 interface Command Using the brief Keyword

The following is sample output from the **show ipv6 interface**command when entered with the **brief** keyword:

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
Ethernet0                  [up/up]
    unassigned
Ethernet1                  [up/up]
    2001:0DB8:1000:/29
Ethernet2                  [up/up]
    2001:0DB8:2000:/29
Ethernet3                  [up/up]
    2001:0DB8:3000:/29
Ethernet4                  [up/down]
    2001:0DB8:4000:/29
Ethernet5                  [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8
Interface         Status                IPv6 Address
Ethernet0         up                    3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1         up                    unassigned
Fddi0             up                    3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0           administratively down unassigned
Serial1           administratively down unassigned
Serial2           administratively down unassigned
Serial3           administratively down unassigned
Tunnel0           up                    unnumbered (Ethernet0)
Tunnel1           up                    3FFE:700:20:1::12
```

IPv6 Interface with ND Prefix Configured

This sample output shows the characteristics of an interface that has generated a prefix from a local IPv6 prefix pool:

```
Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
 ipv6 address 2001:0DB8::1/64
 ipv6 address 2001:0DB8::2/64
 ipv6 nd prefix 2001:0DB8:2::/64
 ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
```

```
       N - Not advertised, C - Calendar
     default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD  2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P    2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

The default prefix shows the parameters that are configured using the ipv6 nd prefix default command.

IPv6 Interface with DRP Configured

This sample output shows the state of the DRP preference value as advertised by this device through an interface:

```
Device# show ipv6 interface gigabitethernet 0/1
  GigabitEthernet0/1 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::130
    Description: Management network (dual stack)
    Global unicast address(es):
      FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:130
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds
    ND advertised 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
    ND advertised default router preference is Low
    Hosts use stateless autoconfig for addresses.
```

IPv6 Interface with HSRP Configured

When HSRP IPv6 is first configured on an interface, the interface IPv6 link-local address is marked unactive (UNA) because it is no longer advertised, and the HSRP IPv6 virtual link-local address is added to the virtual link-local address list with the UNA and tentative DAD (TEN) attributes set. The interface is also programmed to listen for the HSRP IPv6 multicast address.

This sample output shows the status of UNA and TEN attributes, when HSRP IPv6 is configured on an interface:

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [UNA/TEN]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
  MTU is 1500 bytes
```

```
  ICMP error messages limited to one every 100 milliseconds
  ND DAD is enabled, number of DAD attempts: 1
```

After the HSRP group becomes active, the UNA and TEN attributes are cleared, and the overly optimistic DAD (OOD) attribute is set. The solicited node multicast address for the HSRP virtual IPv6 address is also added to the interface.

This sample output shows the status of UNA, TEN and OOD attributes, when HSRP group is activated:

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [OPT]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
    FF02::1:FFA0:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
```

The table below describes additional significant fields shown in the displays for the **show ipv6 interface** command with HSRP configured.

Table 73: show ipv6 interface Command with HSRP Configured Field Descriptions

Field	Description
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	The interface IPv6 link-local address is marked UNA because it is no longer advertised.
FE80::205:73FF:FEA0:1 [UNA/TEN]	The virtual link-local address list with the UNA and TEN attributes set.
FF02::66	HSRP IPv6 multicast address.
FE80::205:73FF:FEA0:1 [OPT]	HSRP becomes active, and the HSRP virtual address marked OPT.
FF02::1:FFA0:1	HSRP solicited node multicast address.

IPv6 Interface with Minimum RA Interval Configured

When you enable Mobile IPv6 on an interface, you can configure a minimum interval between IPv6 router advertisement (RA) transmissions. The **show ipv6 interface** command output reports the minimum RA interval, when configured. If the minimum RA interval is not explicitly configured, then it is not displayed.

In the following example, the maximum RA interval is configured as 100 seconds, and the minimum RA interval is configured as 60 seconds on Ethernet interface 1/0:

```
Device(config-if)# ipv6 nd ra-interval 100 60
```

Subsequent use of the **show ipv6 interface** then displays the interval as follows:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

In the following example, the maximum RA interval is configured as 100 milliseconds (ms), and the minimum RA interval is configured as 60 ms on Ethernet interface 1/0:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 milliseconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The table below describes additional significant fields shown in the displays for the **show ipv6 interface** command with minimum RA interval information configured.

Table 74: show ipv6 interface Command with Minimum RA Interval Information Configuration Field Descriptions

Field	Description
ND router advertisements are sent every 60 to 100 seconds	ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 seconds, and the maximum value is 100 seconds.
ND router advertisements are sent every 60 to 100 milliseconds	ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 ms, and the maximum value is 100 ms.

Related Commands

Command	Description
ipv6 nd prefix	Configures which IPv6 prefixes are included in IPv6 router advertisements.
ipv6 nd ra interval	Configures the interval between IPv6 RA transmissions on an interface.
show ip interface	Displays the usability status of interfaces configured for IP.

IPv6 Commands: show ipv6 lo to show ipv6 mt

show ipv6 local pool

To display information about any defined IPv6 address pools, use the **show ipv6 local pool** command in privileged EXEC mode.

show ipv6 local pool [*poolname* [**cache**]]

Syntax Description

poolname	(Optional) User-defined name for the local address pool.
cache	(Optional) Indicates that cache statistics are to be included in the output display

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

If you omit the *poolname*argument, the command displays a generic list of all defined address pools and the IP addresses that belong to them. If you specify the *poolname* argument, the command displays detailed information about that pool.

Examples

The following command displays IPv6 prefix pool information, which includes cache statistics:

```
Router# show ipv6 local pool mypool
Prefix is 2001:0DB8::/29 assign /64 prefix
2 entries in use, 254 available, 0 rejected
0 entries cached, 1000 maximum

User           Prefix                Interface
joe            3FFE:FFFF:A::/64       Vi1
john           3FFE:FFFF:A:1::/64     Vi2
```

The following command displays IPv6 prefix pool information for all prefix pools:

```
Router# show ipv6 local pool

Pool Prefix Free In use
mypool 2001:0DB8::/29 65516 20
myrouter#
myrouter# show ipv6 local pool mypool
Prefix is 1234::/48 assign /64 prefix
20 entries in use, 65516 available, 0 rejected
0 entries cached, 1000 maximum
User Prefix Interface
user1-72b 1234::/64 Vi1.21
user1-72b 1234:0:0:1::/64 Vi1.22
user1-72b 1234:0:0:2::/64 Vi1.23
user1-72b 1234:0:0:3::/64 Vi1.24
user1-72b 1234:0:0:4::/64 Vi1.25
user1-72b 1234:0:0:5::/64 Vi1.26
user1-72b 1234:0:0:6::/64 Vi1.27
user1-72b 1234:0:0:7::/64 Vi1.28
```

```
user1-72b 1234:0:0:8::/64 Vi1.29
user1-72b 1234:0:0:9::/64 Vi1.30
user1-72b 1234:0:0:A::/64 Vi1.31
user1-72b 1234:0:0:B::/64 Vi1.32
user1-72b 1234:0:0:C::/64 Vi1.33
user1-72b 1234:0:0:D::/64 Vi1.34
user1-72b 1234:0:0:E::/64 Vi1.35
user1-72b 1234:0:0:F::/64 Vi1.36
user1-72b 1234:0:0:10::/64 Vi1.37
user1-72b 1234:0:0:11::/64 Vi1.38
user1-72b 1234:0:0:12::/64 Vi1.39
user1-72b 1234:0:0:13::/64 Vi1.40
```

The table below describes the significant fields shown in the displays.

Table 75: show ipv6 local pool Field Descriptions

Field	Description
Scope	The type of access.
Pool	Pool and group names and associations, if created.
Begin	The first IP address in the defined range of addresses in this pool.
End	The last IP address in the defined range of addresses in this pool.
Free	The number of addresses available.
InUse	The number of addresses in use.

Related Commands

Command	Description
ipv6 local pool	Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface.

show ipv6 mfib

To display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB), use the **show ipv6 mfib** command in user EXEC or privileged EXEC mode.

Cisco 3660 Series Routers, Cisco 10000 Series Routers, and Catalyst 6500 Series Routers

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope** | **verbose** *group-address-name* | *ipv6-prefix* / *prefix-length* *source-address-name* | **interface** | **status** | **summary**}]

Cisco 7600 Series Routers

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope** | **verbose** | **interface** | **status** | **summary**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays all forwarding entries and interfaces in the IPv6 MFIB.
linkscope	(Optional) Displays the link-local groups.
verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.
ipv6-prefix	(Optional) The IPv6 network assigned to the interface. The default IPv6 prefix is 128. 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*	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
group-address-name	(Optional) IPv6 address or name of the multicast group.
source-address-name	(Optional) IPv6 address or name of the multicast group.
interface	(Optional) Interface settings and status.
status	(Optional) General settings and status.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.2(18)SXE	Support for this command was added for the Supervisor Engine 720.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(4)T	The **link-local** keyword was added.
12.3(7)T	The *ipv6-prefix* and *prefix-length* arguments were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 mfib** command to display MFIB entries; and forwarding interfaces, and their traffic statistics. This command can be enabled on virtual IP (VIP) if the router is operating in distributed mode.

A forwarding entry in the MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces. The table below describes the MFIB forwarding entries and interface flags.

Table 76: MFIB Entries and Interface Flags

Flag	Description
F	Forward--Data is forwarded out of this interface.
A	Accept--Data received on this interface is accepted for forwarding.
IC	Internal copy--Deliver to the router a copy of the packets received or forwarded on this interface.
NS	Negate signal--Reverse the default entry signaling behavior for packets received on this interface.
DP	Do not preserve--When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead).
SP	Signal present--The reception of a packet on this interface was just signaled.
S	Signal--By default, signal the reception of packets matching this entry.

Flag	Description
C	Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source.

Examples

The following example displays the forwarding entries and interfaces in the MFIB. The router is configured for fast switching, and it has a receiver joined to FF05::1 on Ethernet1/1 and a source (2001::1:1:20) sending on Ethernet1/2:

```
Router# show ipv6 mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
   Forwarding: 0/0/0/0, Other: 0/0/0
   Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
   Forwarding: 2/0/100/0, Other: 0/0/0
   Tunnel0 Flags: A NS
   Ethernet1/1 Flags: F NS
     Pkts: 0/2
(2001::1:1:200,FF05::1) Flags:
   Forwarding: 5/0/100/0, Other: 0/0/0
   Ethernet1/2 Flags: A
   Ethernet1/1 Flags: F NS
     Pkts: 3/2
(*,FF10::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
```

The table below describes the significant fields shown in the display.

Table 77: show ipv6 mfib Field Descriptions

Field	Description
Entry Flags	Information about the entry.
Forwarding Counts	Statistics on the packets that are received from and forwarded to at least one interface.
Pkt Count/	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.
Pkts per second/	Number of packets received and forwarded per second.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.

Field	Description
Kbits per second	Bytes per second divided by packets per second divided by 1000.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Interface Flags:	Information about the interface.
Interface Counts:	Interface statistics.

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 specified:

```
Router# show ipv6 mfib FF03:1::1
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A
flag,
            AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
*,FF03:1::1) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel1 Flags:A NS
  GigabitEthernet5/0.25 Flags:F NS
    Pkts:0/0
  GigabitEthernet5/0.24 Flags:F NS
    Pkts:0/0
(5002:1::2,FF03:1::1) Flags:
  Forwarding:71505/0/50/0, Other:42/0/42
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0.19 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.20 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.21 Flags:F NS
    Pkts:238/24
.
.
.
GigabitEthernet5/0.16 Flags:F NS
Pkts:71628/24
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 and a source address of 5002:1::2 specified:

```
Router# show ipv6 mfib FF03:1::1 5002:1::2

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
```

```
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5002:1::2,FF03:1::1) Flags:
   Forwarding:71505/0/50/0, Other:42/0/42
   GigabitEthernet5/0 Flags:A
   GigabitEthernet5/0.19 Flags:F NS
     Pkts:239/24
   GigabitEthernet5/0.20 Flags:F NS
     Pkts:239/24
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:71628/24
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 and a default prefix of 128:

```
Router# show ipv6 mfib FF03:1::1/128
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03:1::1) Flags:C
   Forwarding:0/0/0/0, Other:0/0/0
   Tunnel1 Flags:A NS
   GigabitEthernet5/0.25 Flags:F NS
     Pkts:0/0
   GigabitEthernet5/0.24 Flags:F NS
     Pkts:0/0
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:0/0
```

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FFE0 and a prefix of 15:

```
Router# show ipv6 mfib FFE0::/15
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FFE0::/15) Flags:D
   Forwarding:0/0/0/0, Other:0/0/0
```

The following example shows output of the **show ipv6 mfib** command used with the **verbose** keyword. It shows forwarding entries and interfaces in the MFIB and additional information such as the MAC encapsulation header and platform-specific information.

```
Router# show ipv6 mfib ff33::1:1 verbose
```

```
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry,HB - Bridge entry,HD - NonRPF Drop entry,
                NP - Not platform switchable,RPL - RPF-ltl linkage,
                MCG - Metset change,ERR - S/w Error Flag,RTY - In RetryQ,
                LP - L3 pending,MP - Met pending,AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
   RP Forwarding: 0/0/0/0, Other: 0/0/0
   LC Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwd:   0/0/0/0, Other: NA/NA/NA
   Slot 6: HW Forwarding: 0/0, Platform Flags:  HF RPL
   Slot 1: HW Forwarding: 0/0, Platform Flags:  HF RPL
   Vlan10 Flags: A
   Vlan30 Flags: F NS
     Pkts: 0/0/0 MAC: 33330001000100D0FFFE180086DD
```

The table below describes the fields shown in the display.

Table 78: show ipv6 mfib verbose Field Descriptions

Field	Description
Platform flags	Information about the platform.
Platform per slot HW-Forwarding Counts	Total number of packets per bytes forwarded.

Related Commands

Command	Description
show ipv6 mfib active	Displays the rate at which active sources are sending to multicast groups.
show ipv6 mfib count	Displays summary traffic statistics from the MFIB about the group and source.
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.
show ipv6 mfib status	Displays the general MFIB configuration and operational status.
show ipv6 mfib summary	Displays summary information about the number of IPv6 MFIB entries (including link-local groups) and interfaces.

show ipv6 mfib active

To display the rate at which active sources are sending to multicast groups, use the **show ipv6 mfib active** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope**}] **active** [*kbps*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to linkscope (reserved) groups.
kbps	(Optional) Kilobits per second.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 mfib active** command to display MFIB entries actively used to forward packets. In many cases, it is useful to provide the optional *kbps* argument to limit the set of entries displayed to the ones that are forwarding an amount of traffic larger or equal to the amount set by the *kbps* argument.

Examples

The following example displays statistics on the rate at which active IP multicast sources are sending information. The router is switching traffic from 2001::1:1:200 to FF05::1:

```
Router# show ipv6 mfib active
Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001::1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

The table below describes the significant fields shown in the display.

Table 79: show ipv6 mfib active Field Descriptions

Field	Description
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Rate...kbps	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Refer to the platform documentation for more information.

show ipv6 mfib count

To display summary traffic statistics from the IPv6 Multicast Forwarding Information Base (MFIB) about multicast sources and groups, use the **show ipv6 mfib count** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope**}] **count**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to linkscope (reserved) groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 mfib count** command to display the average packet size and data rate in kilobits per seconds.

Examples

The following example displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to both reserved and nonreserved groups:

```
Router# show ipv6 mfib all count
```

show ipv6 mfib global

To display information from the IPv6 Multicast Forwarding Information Base (MFIB) global table, use the **show ipv6 mfib active** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope**}] **global**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays information in the IPv6 MFIB global table for both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays information in the IPv6 MFIB global table for linkscope groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If no optional keywords or arguments are entered, global table information in the IPv6 MFIB associated with nonlinkscope multicast groups are displayed.

Examples

The following example enables you to display IPv6 MFIB global table information:

```
Router# show ipv6 mfib global
```

show ipv6 mfib instance

To display information about an IPv6 Multicast Forwarding Information Base (MFIB) table instance, use the **show ipv6 mfib instance**command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope**}] **instance**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays all information about a.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv6 MFIB about multicast sources sending to linkscope (reserved) groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Examples

The following example enables you to display IPv6 MFIB instance information:

```
Router# show ipv6 mfib instance
```

show ipv6 mfib interface

To display information about IPv6 multicast-enabled interfaces and their forwarding status, use the **show ipv6 mfib interface** command in user EXEC or privileged EXEC mode.

show ipv6 mfib interface

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 mfib interface** command displays the Multicast Forwarding Information Base (MFIB) interfaces and in what switching mode each MFIB has been configured.

Examples

The following example displays information about IPv6 multicast-enabled interfaces and their forwarding status. The router is configured for fast switching.

```
Router# show ipv6 mfib interface
IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                             [configured,available]
Ethernet1/1          up      [yes       ,yes      ]
Ethernet1/2          up      [yes       ,?        ]
Tunnel0              up      [yes       ,?        ]
Tunnel1              up      [yes       ,?        ]
```

The table below describes the significant fields shown in the display.

Table 80: show ipv6 mfib interface Field Descriptions

Field	Description
MFIB interface	Specifies the MFIB interface.
Status	Specifies the status of the MFIB interface.
CEF-based output	Provides information on the Cisco Express Forwarding-based output of the MFIB interface.

show ipv6 mfib route

To display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB) without packet header information and forwarding counters, use the **show ipv6 mfib route**command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] [{**all** | **linkscope**}] **route**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
all	(Optional) Displays the forwarding entries and interfaces in the IPv6 MFIB for both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays the forwarding entries and interfaces in the IPv6 MFIB for linkscope (reserved) groups.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was modified. The **link-local** keyword was changed to **linkscope**.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
Cisco IOS XE Release 3.2S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Examples

The following example enables you to display IPv6 MFIB instance information:

```
Router# show ipv6 mfib instance
```

show ipv6 mfib status

To display the general Multicast Forwarding Information Base (MFIB) configuration and operational status, use the **show ipv6 mfib status** command in user EXEC or privileged EXEC mode.

show ipv6 mfib status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 mfib status** to find such information as whether or not MFIB is enabled and running.

Examples

The following example displays MFIB information:

```
Router# show ipv6 mfib status
IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: not running
    Notes: MFIB not running because multicast routing is disabled
```

The table below describes the significant fields shown in the displays.

Table 81: show ipv6 mfib status Field Descriptions

Field	Description
Configuration status: enabled	MFIB is enabled on the device.
Operational status: not running	Although MFIB is enabled on the device, it is not running.
Notes:	Information about MFIB configuration and operational status.

show ipv6 mfib summary

To display summary information about the number of IPv6 Multicast Forwarding Information Base (MFIB) entries (including link-local groups) and interfaces, use the **show ipv6 mfib summary** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**vrf** *vrf-name*] **summary**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 mfib summary** command shows the IP multicast routing table in abbreviated form. The command displays only the number of MFIB entries, the number of (*, G) and (S, G) entries, and the number of MFIB interfaces specified.

The **show ipv6 mfib summary** command counts all entries, including link-local entries.

Examples

The following example displays summary information about the number of IPv6 MFIB entries and interfaces:

```
Router# show ipv6 mfib summary

IPv6 MFIB summary:
  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17     total MFIB interfaces
```

The table below describes the significant fields shown in the display.

Table 82: show ipv6 mfib summary Field Descriptions

Field	Description
54 total entries	Total number of MFIB entries, including the number of (*, G) and (S, G) entries.
17 total MFIB interfaces	Sum of all the MFIB interfaces in all the MFIB entries.

show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the **show ipv6 mld groups** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **groups** [**link-local**] [{*group-namegroup-address*}] [*interface-type interface-number*] [{**detail** | **explicit**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
interface-type interface-number	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about individual sources.
explicit	(Optional) Displays information about the hosts being explicitly tracked on each interface for each group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.3(7)T	The **explicit** keyword was added.
12.2(25)S	The link-local and **explicit** keywords were added.
12.4(2)T	Information about MLD state limits was added to the command output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Release	Modification
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

If you omit all optional arguments, the **show ipv6 mld groups** command displays by group address and interface type and number all directly connected multicast groups, including link-local groups (where the **link-local** keyword is not available) used.

Examples

The following is sample output from the **show ipv6 mld groups** command. It shows all of the groups joined by Fast Ethernet interface 2/1, including link-local groups used by network protocols.

```
Router# show ipv6 mld groups FastEthernet 2/1
MLD Connected Group Membership
Group Address          Interface           Uptime        Expires
FF02::2                FastEthernet2/1     3d18h         never
FF02::D                FastEthernet2/1     3d18h         never
FF02::16               FastEthernet2/1     3d18h         never
FF02::1:FF00:1         FastEthernet2/1     3d18h         00:00:27
FF02::1:FF00:79        FastEthernet2/1     3d18h         never
FF02::1:FF23:83C2      FastEthernet2/1     3d18h         00:00:22
FF02::1:FFAF:2C39      FastEthernet2/1     3d18h         never
FF06:7777::1           FastEthernet2/1     3d18h         00:00:26
```

The following is sample output from the **show ipv6 mld groups** command using the **detail** keyword:

```
Router# show ipv6 mld groups detail
Interface:      Ethernet2/1/1
Group:          FF33::1:1:1
Uptime:         00:00:11
Router mode:    INCLUDE
Host mode:      INCLUDE
Last reporter:  FE80::250:54FF:FE60:3B14
Group source list:
Source Address                          Uptime    Expires   Fwd  Flags
2004:4::6                               00:00:11  00:04:08  Yes  Remote Ac 4
```

The following is sample output from the **show ipv6 mld groups**command using the **explicit** keyword:

```
Router# show ipv6 mld groups explicit
Ethernet1/0, FF05::1
    Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
    Host Address                        Uptime   Expires
    FE80::A8BB:CCFF:FE00:800            00:43:11 00:03:17
    Mode:EXCLUDE
Ethernet1/0, FF05::6
    Up:00:42:22 INCLUDE(1/0) Exp:not used
    Host Address                        Uptime   Expires
    FE80::A8BB:CCFF:FE00:800            00:42:22 00:03:17
    Mode:INCLUDE
        300::1
        300::2
        300::3
Ethernet1/0 - Interface
ff05::1 - Group address
```

```
Up:Uptime for the group
EXCLUDE/INCLUDE - The mode the group is in on the router.
(0/1) (1/0) - (Number of hosts in INCLUDE mode/Number of hosts in EXCLUDE moe)
Exp:Expiry time for the group.
FE80::A8BB:CCFF:FE00:800 - Host ipv6 address.
00:43:11 - Uptime for the host.
00:03:17 - Expiry time for the host
Mode:INCLUDE/EXCLUDE - Mode the Host is operating in.
300::1, 300::2, 300::3 - Sources that the host has joined in the above specified mode.
```

The table below describes the significant fields shown in the display.

Table 83: show ipv6 mld groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long (in hours, minutes, and seconds) this multicast group has been known.
Expires	How long (in hours, minutes, and seconds) until the entry is removed from the MLD groups table. The expiration timer shows "never" if the router itself has joined the group, and the expiration timer shows "not used" when the router mode of the group is INCLUDE. In this situation, the expiration timers on the source entries are used.
Last reporter:	Last host to report being a member of the multicast group.
Flags Ac 4	Flags counted toward the MLD state limits configured.

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

show ipv6 mld groups summary

To display the number of (*, G) and (S, G) membership reports present in the Multicast Listener Discovery (MLD) cache, use the **show ipv6 mld groups summary** command in user EXEC or privileged EXEC mode.

show ipv6 mld groups summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 mld groups summary** command displays the number of directly connected multicast groups (including link-local groups).

Examples

The following is sample output from the **show ipv6 mld groups summary**command:

```
Router# show ipv6 mld groups summary
MLD Route Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 0
```

The table below describes the significant fields shown in the display.

Table 84: show ipv6 mld groups summary Field Descriptions

Field	Description
No. of (*,G) routes = 5	Displays the number of groups present in the MLD cache.

Field	Description
No. of (S,G) routes = 0	Displays the number of include and exclude mode sources present in the MLD cache.

show ipv6 mld host-proxy

To display IPv6 MLD host proxy information, use the **show ipv6 mld host-proxy** command in user EXEC or privileged EXEC mode.

show ipv6 mld host-proxy [*interface-type interface-number*] [**group** [*group-address*]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.
group	(Optional) Displays a list of group entries for which the specified interface is acting as a proxy interface.
group-address	(Optional) Specified group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The show ipv6 mld host-proxy command displays MLD proxy information. When this command is used with the *interface-type interface-number*arguments, interface details such as interface state, IPv6 address, MLD state, etc., are displayed. If an interface is not specified, the **show ipv6 mld host-proxy** command displays all active proxy interfaces on the router.

The show ipv6 mld host-proxy command when used with the *interface-type interface-number*arguments and the **group** keyword displays information about group entries for which interface is acting as a proxy interface. If the *group-address* argument is specified, it display the group information for specified group.

Examples

The following example displays IPv6 MLD proxy information for the Ethernet 0/0 interface:

```
Router# show ipv6 mld host-proxy Ethernet0/0
Ethernet0/0 is up, line protocol is up
  Internet address is FE80::34/64
MLD is enabled on interface
  MLD querying router is FE80::12, Version: MLDv2
  Current MLD host version is 2
  MLD max query response time is 10 seconds
Number of MLD Query sent on interface : 10
Number of MLD Query received on interface : 20
Number of MLDv1 report sent : 5
Number of MLDv2 report sent : 10
Number of MLDv1 leave sent : 0
Number of MLDv2 leave sent : 1
```

The table below describes the significant fields shown in the display.

Table 85: show ipv6 mld host-proxy Field Descriptions

Field	Description
Ethernet0/0 is up, line protocol is up	State of the specified interface.
Internet address is FE80::34/64	IPv6 address of the specified interface.
MLD is enabled on interface	State of MLD on the interface, whether enabled or disabled.
MLD querying router is FE80::12, Version: MLDv2	IPv6 address and MLD version of the querying router.
Current MLD host version is 2	Configured MLD host version.
MLD max query response time is 10 seconds	Maximum allowed response time for the query.
Number of MLD Query sent on interface: 10	Number of MLD queries sent from the interface.
Number of MLD Query received on interface: 20	Number of MLD queries received on the interface.
Number of MLDv1 report sent : 5	Number of MLDv1 membership reports sent.
Number of MLDv2 report sent : 10	Number of MLDv2 membership reports sent.
Number of MLDv1 leave sent : 0	Number of MLDv1 leave reports sent.
Number of MLDv2 leave sent : 1	Number of MLDv2 leave reports sent.

The following example provides information about a group entry for the Ethernet 0/0 proxy interface:

```
Router# show ipv6 mld host-proxy Ethernet0/0 group
Group:               FF5E::12
Uptime:             00:00:07
Group mode:     INCLUDE
Version             MLDv2
Group source list:
  Source Address        Uptime
            5000::2                     00:00:07
            2000::2                     00:01:15
Group:               FF7E::21
Uptime:             00:02:07
Group mode:     EXCLUDE
Version              MLDv2
Group source list: Empty
```

The table below describes the significant fields shown in the display.

Table 86: show ipv6 mld host-proxy Field Descriptions

Field	Description
Group: FF5E::12	The IPv6 address of the group.
Uptime: 00:00:07	The length of time the group has been active.
Group mode: INCLUDE	The group mode.

Field	Description
Version MLDv2	The MLD version on the proxy interface.
Group source list:	Information on the group source list.

Related Commands

Command	Description
ipv6 mld host-proxy	Enables the MLD proxy feature.
ipv6 mld host-proxy interface	Enables the MLD proxy feature on a specified interface on an RP.

show ipv6 mld interface

To display multicast-related information about an interface, use the **show ipv6 mld interface** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **interface** [*type number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
type number	(Optional) Interface type and number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.4(2)T	Information about MLD state limits was added to the command output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

If you omit the optional *type* and *number* arguments, the **show ipv6 mld interface** command displays information about all interfaces.

Examples

The following is sample output from the **show ipv6 mld interface** command for Ethernet interface 2/1/1:

```
Router# show ipv6 mld interface Ethernet 2/1/1
Global State Limit : 2 active out of 2 max
Loopback0 is administratively down, line protocol is down
  Internet address is ::/0
```

```
.
.
.
Ethernet2/1/1 is up, line protocol is up
  Internet address is FE80::260:3EFF:FE86:5649/10
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Interface State Limit : 2 active out of 3 max
  State Limit permit access list:
  MLD activity: 83 joins, 63 leaves
  MLD querying router is FE80::260:3EFF:FE86:5649 (this system)
```

The table below describes the significant fields shown in the display.

Table 87: show ipv6 mld interface Field Descriptions

Field	Description
Global State Limit: 2 active out of 2 max	Two globally configured MLD states are active.
Ethernet2/1/1 is up, line protocol is up	Interface type, number, and status.
Internet address is...	Internet address of the interface and subnet mask being applied to the interface.
MLD is enabled in interface	Indicates whether Multicast Listener Discovery (MLD) has been enabled on the interface with the **ipv6 multicast-routing**command.
Current MLD version is 2	The current MLD version.
MLD query interval is 125 seconds	Interval (in seconds) at which the Cisco IOS software sends MLD query messages, as specified with the **ipv6 mld query-interval**command.
MLD querier timeout is 255 seconds	The length of time (in seconds) before the router takes over as the querier for the interface, as specified with the **ipv6 mld query-timeout**command.
MLD max query response time is 10 seconds	The length of time (in seconds) that hosts have to answer an MLD Query message before the router deletes their group, as specified with the **ipv6 mld query-max-response-time** command.
Last member query response interval is 1 seconds	Used to calculate the maximum response code inserted in group and source-specific query. Also used to tune the "leave latency" of the link. A lower value results in reduced time to detect the last member leaving the group.
Interface State Limit : 2 active out of 3 max	Two out of three configured interface states are active.
State Limit permit access list: change	Activity for the state permit access list.

Field	Description
MLD activity: 83 joins, 63 leaves	Number of groups joins and leaves that have been received.
MLD querying router is FE80::260:3EFF:FE86:5649 (this system)	IPv6 address of the querying router.

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.

show ipv6 mld snooping

To display Multicast Listener Discovery version 2 (MLDv2) snooping information, use the **show ipv6 mld snooping** command in privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **snooping** {**explicit-tracking vlan** *vlan* | **mrouter** [**vlan** *vlan*] | **report-suppression vlan** *vlan* | **statistics vlan** *vlan*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
explicit-tracking vlan *vlan*	Displays the status of explicit host tracking.
mrouter	Displays the multicast router interfaces on an optional VLAN.
vlan *vlan*	(Optional) Specifies the VLAN number on the multicast router interfaces.
report-suppression vlan *vlan*	Displays the status of the report suppression.
statistics vlan *vlan*	Displays MLD snooping information on a VLAN.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

You can enter the **show ipv6 mld snooping mrouter** command without arguments to display all the multicast router interfaces.

Examples

This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                      Interface    Reporter        Filter_mode
------------------------------------------------------------------------
10.1.1.1/226.2.2.2                Vl25:1/2     10.27.2.3       INCLUDE
10.2.2.2/226.2.2.2                Vl25:1/2     10.27.2.3       INCLUDE
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show
ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+----------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
```

This example shows the MLD snooping statistics information for VLAN 25:

```
Router# show ipv6 mld
 snooping statistics interface vlan 25
Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
```

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 snooping globally.
ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
ipv6 mld snooping querier	Enables the MLDv2 snooping querier.
ipv6 mld snooping report-suppression	Enables report suppression on a VLAN.

show ipv6 mld ssm-map

To display Source Specific Multicast (SSM) mapping information, use the **show ipv6 mld ssm-map static**command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **ssm-map** [*source-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
source-address	(Optional) Source address associated with an MLD membership for a group identified by the access list.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

If the optional *source-address* argument is not used, all SSM mapping information is displayed.

Examples

The following example shows all SSM mappings for the router:

```
Router# show ipv6 mld ssm-map
SSM Mapping  : Enabled
DNS Lookup   : Enabled
```

The following examples show SSM mapping for the source address 2001:0DB8::1:

```
Router# show ipv6 mld ssm-map 2001:0DB8::1
 Group address  : 2001:0DB8::1
 Group mode ssm : TRUE
 Database       : STATIC
 Source list    : 2001:0DB8::2
                  2001:0DB8::3
Router# show ipv6 mld ssm-map 2001:0DB8::2
 Group address  : 2001:0DB8::2
 Group mode ssm : TRUE
 Database       : DNS
 Source list    : 2001:0DB8::3
                  2001:0DB8::1
```

The table below describes the significant fields shown in the displays.

Table 88: show ipv6 mld ssm-map Field Descriptions

Field	Description
SSM Mapping	The SSM mapping feature is enabled.
DNS Lookup	The DNS lookup feature is automatically enabled when the SSM mapping feature is enabled.
Group address	Group address identified by a specific access list.
Group mode ssm : TRUE	The identified group is functioning in SSM mode.
Database : STATIC	The router is configured to determine source addresses by checking static SSM mapping configurations.
Database : DNS	The router is configured to determine source addresses using DNS-based SSM mapping.
Source list	Source address associated with a group identified by the access list.

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counters, use the **show ipv6 mld traffic** command in user EXEC or privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 mld traffic**commandto check if the expected number of MLD protocol messages have been received and sent.

Examples

The following example displays the MLD protocol messages received and sent.

```
Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21
                              Received     Sent
Valid MLD Packets                3           1
Queries                          1           0
Reports                          2           1
Leaves                           0           0
Mtrace packets                   0           0
Errors:
Malformed Packets                            0
Bad Checksums                                0
Martian source                               0
Packets Received on MLD-disabled Interface   0
```

The table below describes the significant fields shown in the display.

Table 89: show ipv6 mld traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid MLD packets	Number of valid MLD packets received and sent.
Queries	Number of valid queries received and sent.
Reports	Number of valid reports received and sent.
Leaves	Number of valid leaves received and sent.
Mtrace packets	Number of multicast trace packets received and sent.
Errors	Types of errors and the number of errors that have occurred.

show ipv6 mobile binding

To display information about the binding cache, use the **show ipv6 mobile binding** command in user EXEC or privileged EXEC mode.

show ipv6 mobile binding [{**care-of-address** *address* | **home-address** *address* | *interface-type interface-number*}]

Syntax Description

care-of-address	(Optional) Provides information about the mobile node's current location.
address	(Optional) Current address of the mobile node.
home-address	(Optional) IPv6 address is assigned to the mobile node within its home subnet prefix on its home link.
interface-type interface-number	(Optional) Interface type and number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	Command output was updated to display the tunnel interface and the tunnel end point details.

Usage Guidelines

The **show ipv6 mobile binding** command displays details of all bindings that match all search criteria. If no optional keywords or arguments are specified, all bindings are displayed.

Examples

The following example displays information about the binding cache:

```
Router# show ipv6 mobile binding
Mobile IPv6 Binding Cache Entries:
  2001:1::8
    via care-of address 2001:2::1
    home-agent 2001:1::2
    state ACTIVE, sequence 1, flags AHrlK
    lifetime:remaining 1023 (secs), granted 1024 (secs), requested 1024 (secs)
    interface Ethernet1/3
    0 tunneled, 0 reversed tunneled
Selection matched 1 bindings
```

The following example displays information about the tunnel interface and the tunnel end point details:

```
Router# show ipv6 mobile bindings
Tunnel Interface: tunnel0
Tunnel Source 2001:0DB1:1:1
Tunnel Destination: 2001:0DB1:2:1
Input: 20 packets, 1200 bytes, 0 drops
Output: 20 packets, 1200 bytes, 0 drops
```

The table below describes the significant fields shown in the displays.

Table 90: show ipv6 mobile binding Field Descriptions

Field	Description
2001:1::8	Home IPv6 address of the mobile node.
via care-of address 2001:2::1	Care-of address of the mobile node.
home-agent 2001:1::2	Home-agent address
state ACTIVE, sequence 1, flags AHrlK	• State: State of the mobile binding. • Sequence number. • Flags: Services requested by mobile node. The mobile node requests these services by setting bits in the registration request. Uppercase characters denote bit set.
lifetime:remaining 1023 (secs), granted 1024 (secs), requested 1024 (secs)	• Remaining: The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the home agent. • Granted: The lifetime granted to the mobile node for this registration. Number of seconds in parentheses. • Requested: The lifetime requested by the mobile node for this registration. Number of seconds in parentheses.
interface Ethernet1/3	The interface being used.
0 tunneled, 0 reversed tunneled	Number of bindings tunneled and reverse tunneled.
Selection matched 1 bindings	Total number of mobility bindings that were matched.
Tunnel Interface	The tunnel interface being used.
Tunnel Source	Tunnel source IPv6 address.
Tunnel Destionation	Tunnel destination IPv6 address.
Input	Number of packets in.
Output	Number of packets out.

Related Commands

binding	Configures binding options for the Mobile IPv6 home agent feature in home-agent configuration mode.
ipv6 mobile home-agent (interface configuration)	Initializes and starts the Mobile IPv6 home agent on a specific interface.

show ipv6 mobile globals

To display global Mobile IPv6 parameters, use the **show ipv6 mobile globals**command in user EXEC or privileged EXEC mode.

show ipv6 mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	Command output was updated to show the Mobile IPv6 tunnel information on the home agent.

Usage Guidelines

The **show ipv6 mobile globals** command displays the values of all global configuration parameters associated with Mobile IPv6 and lists the interfaces on which home agent functionality is operating.

Examples

In the following example, the **show ipv6 mobile globals** command displays the binding parameters:

```
Router# show ipv6 mobile globals

Mobile IPv6 Global Settings:
  1 Home Agent service on following interfaces:
    Ethernet1/2
  Bindings:
    Maximum number is unlimited.
    1 bindings are in use
    1 bindings peak
    Binding lifetime permitted is 262140 seconds
    Recommended refresh time is 300 seconds
```

In the following example, the **show ipv6 mobile globals** command displays the Mobile IPv6 tunnel information parameters on the home agent:

```
Router# show ipv6 mobile globals
Tunnel Encapsulation Mode: IPv6/IPv6
ICMP Unreachable for tunnel interfaces <enabled/disabled>
Tunnel Path MTU Discovery: <enabled/disabled>
```

The table below describes the significant fields shown in the displays.

Table 91: show ipv6 mobile globals Field Descriptions

Field	Description
1 Home Agent service on following interfaces: Ethernet1/2	Interface on which the home agent service is enabled.

Field	Description
Bindings:	Information on bindings.
Maximum number is unlimited.	The amount of bindings allowed on the home agent.
1 bindings are in use.	How many bindings are being used.
1 bindings peak	The maximum number of bindings that have been used in this session.
Binding lifetime permitted is 262140 seconds	The configured binding lifetime.
Recommended refresh time is 300 seconds	The configured refresh time.
Tunnel Encapsulation Mode:	Tunnel encapsulation type.
ICMP Unreachable for tunnel interfaces	Enabled or disabled.
Tunnel Path MTU Discovery:	Enabled or disabled.

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 mobile node.
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
host group	Creates a host configuration in Mobile IPv6.

show ipv6 mobile home-agents

To display local and discovered neighboring home agents, use the **show ipv6 mobile home-agents**command in user EXEC or privileged EXEC mode.

show ipv6 mobile home-agents [*interface-type interface-number* [*prefix*]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.
prefix	(Optional) IPv6 address prefix of the care-of address or the home address of neighboring agents.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile home-agents**command displays information about local and discovered neighboring home agents. You can choose to display information on a specified interface using the optional *interface-type* and *interface-number* arguments, and you can further choose to display only those addresses that match the optional *prefix* argument.

If no argument or keyword is entered, the home agent list for each interface on which the router is acting as a home agent is displayed. Each list is displayed in decreasing order of preference.

Examples

In the following example, the fact that no neighboring mobile home agents were found is displayed:

```
Router# show ipv6 mobile home-agents
Home Agent information for Ethernet1/3
  Configured:
    FE80::20B:BFFF:FE33:501F
    preference 0 lifetime 1800
      global address 2001:0DB8:1::2/64
  Discovered Home Agents:
    FE80::4, last update 0 min
    preference 0 lifetime 1800
      global address 2001:0DB8:1::4/64
```

The table below describes the significant fields shown in the display.

Table 92: show ipv6 mobile home-agents Field Descriptions

Field	Description
Home Agent information for Ethernet1/3	The interface on which the home agent is configured.
Configured: FE80::20B:BFFF:FE33:501F	The IPv6 address on which the home agent is configured.

Field	Description
preference 0 lifetime 1800	The configured home agent preference and lifetime.
global address 2001:0DB8:1::2/64	The configured global address.
Discovered Home Agents: FE80::4, last update 0 min preference 0 lifetime 1800 global address 2001:0DB8:1::4/64	The address and configuration information about discovered home agents.

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.

show ipv6 mobile host groups

To display information about IPv6 mobile host groups, use the **show ipv6 mobile host groups**command in user EXEC or privileged EXEC mode.

show ipv6 mobile host groups [*profile-name*]

Syntax Description

profile-name	(Optional) Host group profile name.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile host groups**command lists the configuration of all configured host groups. To display information about a specific host group, use the optional *profile-name* keyword.

Examples

In the following example, information about a host group named localhost is displayed:

```
Router# show ipv6 mobile host groups
Mobile IPv6 Host Configuration
Mobile Host List:
Host Group Name: localhost
    NAI: sai@cisco.com
    Address: CAB:C0:CA5A:CA5A::CA5A
    Security Association Entry:
      SPI: (Hex: 501) (Decimal Int: 1281)
      Key Format: Hex    Key: baba
      Algorithm: HMAC_SHA1
      Replay Protection: On    Replay Window: 6 secs
```

The table below describes the significant fields shown in the display.

Table 93: show ipv6 mobile host groups Field Descriptions

Field	Description
Host Group Name: localhost	Configuration information about the host group named localhost to follow.
NAI: sai@cisco.com	Network access identifier (NAI) for localhost host group.
Address: 2001:0DB8:CA5A:CA5A::CA5A	IPv6 address for localhost host group.
Security Association Entry:	Security association for the host group named localhost to follow.
SPI: (Hex: 501) (Decimal Int: 1281)	SPI for localhost.

Field	Description
Key Format: Hex Key: baba	Key format and name for localhost.
Algorithm: HMAC_SHA1	Authentication algorithm.
Replay Protection: On Replay Window: 6 secs	Replay protection is activated, and the number of seconds that the router uses for replay protection is 6.

Related Commands

Command	Description
address (Mobile IPv6)	Specifies the home address of the IPv6 mobile node.
authentication (Mobile IPv6)	Specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional SPI.
host group	Creates a host group configuration in IPv6 Mobile.
nai	Specifies the NAI for the IPv6 mobile node.
show ipv6 mobile globals	Displays global Mobile IPv6 parameters.

show ipv6 mobile router

To display configuration information and monitoring statistics about the IPv6 mobile router, use the **show ipv6 mobile router**command in user EXEC or privileged EXEC mode.

show ipv6 mobile router [{**running-config** | **status**}]

Syntax Description

running-config	(Optional) Displays IPv6 mobile router running configuration information.
status	(Optional) Displays IPv6 mobile router status information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile router**display includes the mobile router configuration information such as the home address and network mask, home agent, and registration settings, and operational information such as status, tunnel interface, active foreign agent, and care-of address.

Examples

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

```
Router# show ipv6 mobile router

Mobile Reverse Tunnel established
---------------------------------
using Nemo Basic mode
Home Agent: 2001:DB8:2000::2001
CareOf Address: 2001:DB8::A8BB:CCFF:FE01:F611
Attachment Router: FE80::A8BB:CCFF:FE01:F511
Attachment Interface: Ethernet1/1
Home Network: 2001:DB8:2000:0:FDFF:FFFF:FFFF:FFFE/64
Home Address: 2001:DB8:2000::1111
```

The table below describes the significant fields shown in the display.

Table 94: show ipv6 mobile router Field Descriptions

Field	Description
Mobile Reverse Tunnel established	If reverse tunnel is enabled or disabled, this information is displayed or absent, respectively.
using Nemo Basic mode	Type of mode being used by the mobile router.
Home Agent:	Home agent with which the mobile router registers. The mobile router registers only to the home agent with the highest priority when multiple addresses are configured.

Field	Description
CareOf Address:	Care-of address used by the registered mobile router.
Attachment Router:	Attachment point in the foreign network.
Attachment Interface:	Attachment interface used in the foreign network.
Home Network:	IPv6 address of the mobile router home network.
Home Address:	IPv6 address of the mobile router.

show ipv6 mobile traffic

To display information about binding updates received and binding acknowledgments sent, use the **show ipv6 mobile traffic**command in user EXEC or privileged EXEC mode.

show ipv6 mobile traffic

Syntax Description

The command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The show ipv6 mobile traffic command displays counters and other information associated with Mobile IPv6. The following counters are maintained globally across all interfaces:

- Dynamic home agent discovery requests received
- Binding updates received
- Home agent registrations received
- Successful home agent registrations
- Home agent deregistrations (lifetime of zero or care-of address equals home address)
- Home agent registrations rejected, defined in the status as sent in the binding acknowledgment with a separate counter for every reason code defined in the table below, and generated by the implementation
- Time of last registration acceptance
- Time of last registration denial
- Status code for last registration denial
- Binding updates discarded through rate limiting
- Binding acknowledgments discarded through rate limiting
- Binding cache high-water mark, maintained and displayed for registrations

The table below shows possible binding status values and reasons for use of these values.

Table 95: show ipv6 mobile traffic Field Descriptions

Reason Code	Binding Status Value
0	Binding update accepted

Reason Code	Binding Status Value
128	Reason unspecified
129	Administratively prohibited
130	Insufficient resources
131	Home registration not supported
132	Not home subnet
133	Not home agent for this mobile node
134	Duplicate address detection (DAD) failed
135	Sequence number out of window

Examples

In the following example, information about IPv6 Mobile traffic is displayed:

```
Router# show ipv6 mobile traffic

MIPv6 statistics:
  Rcvd: 6477 total
      0 truncated, 0 format errors
      0 checksum errors
    Binding Updates received:6477
      0 no HA option, 0 BU's length
      0 options' length, 0 invalid CoA
  Sent: 6477 generated
    Binding Acknowledgements sent:6477
      6477 accepted (0 prefix discovery required)
      0 reason unspecified, 0 admin prohibited
      0 insufficient resources, 0 home reg not supported
      0 not home subnet, 0 not home agent for node
      0 DAD failed, 0 sequence number
    Binding Errors sent:0
      0 no binding, 0 unknown MH
  Home Agent Traffic:
    6477 registrations, 0 deregistrations
    00:00:23 since last accepted HA registration
    unknown time since last failed HA registration
    unknown last failed registration code
    Traffic forwarded:
      0 tunneled, 0 reversed tunneled
    Dynamic Home Agent Address Discovery:
      1 requests received, 1 replies sent
    Mobile Prefix Discovery:
      0 solicitations received, 0 advertisements sent
```

The table below describes the significant fields shown in the display.

Table 96: show ipv6 mobile traffic Field Descriptions

Field	Description
MIPv6 statistics:	Information about binding updates received by the mobility agent.

Field	Description
Sent:	Information about binding acknowledgments sent by the mobility agent.
Binding Errors sent:	Information about binding errors sent by the mobility agent.
Home Agent Traffic: 6477 registrations, 0 deregistrations	Number of registrations and deregistrations accepted by the home agent.
00:00:23 since last accepted HA registration	Length of time since the last registration was accepted by the home agent.
unknown time since last failed HA registration	Length of time since the last failed registration by the home agent.
unknown last failed registration code	Reason why the registration failed, if it did fail.
Dynamic Home Agent Address Discovery:	Number of dynamic home agent discovery requests received and replies sent.
Mobile Prefix Discovery:	Number of mobile prefix discovery solicitations received and advertisements sent by the home agent.

Related Commands

Command	Description
binding	Configures binding options for the Mobile IPv6 home agent feature in home agent configuration mode.

show ipv6 mobile tunnels

To list the Mobile IPv6 tunnels on the home agent, use the **show ipv6 mobile tunnels**command in user EXEC or privileged EXEC mode.

show ipv6 mobile tunnels [{**summary** | **tunnel** *if-number*}]

Syntax Description

tunnel *if-number*	(Optional) Tunnel interface.
summary	(Optional) Summary of tunnels on the home agent.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 mobile tunnels** command displays active tunnels on the Mobile IPv6 home agent. Use the **summary** keyword to view a summary of all tunnels on the home agent, or the **tunnel***if-number* keyword and argument to view information on a specific tunnel.

Examples

The following example displays information about the Mobile IPv6 tunnels on the home agent:

```
Router# show ipv6 mobile tunnels
Tunnel1:
 Source: 2001:0DB1:1:1
 Destination: 2001:0DB1:2:1
 Encapsulation Mode: IPv6/IPv6
 Egress Interface: Ethernet 1/0
 Switching Mode: Process
 Keep-Alive: Not Supported
 Path MTU Discovery: Enabled
 Input: 20 packets, 1200 bytes, 0 drops
 Output: 20 packets, 1200 bytes, 0 drops
 NEMO Options: Not Supported
```

The table below describes the significant fields shown in the display.

Table 97: show ipv6 mobile tunnels Field Descriptions

Field	Description
Source:	Source IPv6 tunnel address.
Destination:	Destination IPv6 tunnel address.
Encapsulation Mode:	Tunnel encapsulation type.
Egress interface:	Interface used for egress (outgoing packets).

Field	Description
Switching mode:	Type of switching mode used.
Keep-alive:	Supported or not supported.
Path MTU Discovery:	Enabled or disabled.
Input:	Number of packets in.
Output:	Number of packets out.
NEMO Options:	Supported or not supported.

Related Commands

Command	Description
show ipv6 mobile home-agent	Displays local and discovered neighboring home agents.

show ipv6 mrib client

To display information about the clients of the Multicast Routing Information Base (MRIB), use the **show ipv6 mrib client** command in user EXEC or privileged EXEC mode.

show ipv6 mrib [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* **:** *client-id*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
filter	(Optional) Displays information about MRIB flags that each client owns and that each client is interested in.
name	(Optional) The name of a multicast routing protocol that acts as a client of MRIB, such as Multicast Listener Discovery (MLD) and Protocol Independent Multicast (PIM).
client-name **:** *client-id*	The name and ID of a multicast routing protocol that acts as a client of MRIB, such as MLD and PIM. The colon is required.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **filter** keyword to display information about the MRIB flags each client owns and the flags in which each client is interested.

Examples

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

```
Router# show ipv6 mrib client
IP MRIB client-connections
igmp:145        (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3     (connection id 2)
slot 3  mfib ipv6 rp agent:16   (connection id 3)
slot 1  mfib ipv6 rp agent:16   (connection id 4)
slot 0  mfib ipv6 rp agent:16   (connection id 5)
slot 4  mfib ipv6 rp agent:16   (connection id 6)
slot 2  mfib ipv6 rp agent:16   (connection id 7)
```

The table below describes the significant fields shown in the display.

Table 98: show ipv6 mrib client Field Descriptions

Field	Description
igmp:145 (connection id 0) pim:146 (connection id 1) mfib ipv6:3 (connection id 2) mfib ipv6 rp agent:16 (connection id 3)	Client ID (client name:process ID)

show ipv6 mrib route

To display Multicast Routing Information Base (MRIB) route information, use the **show ipv6 mrib route** command in user EXEC or privileged EXEC mode.

show ipv6 mrib [**vrf** *vrf-name*] **route** [{**link-local** | **summary** | [{*sourceaddress-or-name* | *****}] [*groupname-or-address* [*prefix-length*]]}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
summary	(Optional) Displays the number of MRIB entries (including link-local groups) and interfaces present in the MRIB table.
sourceaddress-or-name	(Optional) IPv6 address or name of the source.
*	(Optional) Displays all MRIB route information.
groupname or-address	(Optional) IPv6 address or name of the multicast group.
prefix-length	(Optional) IPv6 prefix length.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

All entries are created by various clients of the MRIB, such as Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), and Multicast Forwarding Information Base (MFIB). The flags on each entry or interface serve as a communication mechanism between various clients of the MRIB. The entries reveal how PIM sends register messages for new sources and the action taken.

The **summary** keyword shows the count of all entries, including link-local entries.

The interface flags are described in the table below.

Table 99: Description of Interface Flags

Flag	Description
F	Forward--Data is forwarded out of this interface
A	Accept--Data received on this interface is accepted for forwarding
IC	Internal copy
NS	Negate signal
DP	Do not preserve
SP	Signal present
II	Internal interest
ID	Internal uninterest
LI	Local interest
LD	Local uninterest
C	Perform directly connected check

Special entries in the MRIB indicate exceptions from the normal behavior. For example, no signaling or notification is necessary for arriving data packets that match any of the special group ranges. The special group ranges are as follows:

- Undefined scope (FFX0::/16)
- Node local groups (FFX1::/16)
- Link-local groups (FFX2::/16)
- Source Specific Multicast (SSM) groups (FF3X::/32).

For all the remaining (usually sparse-mode) IPv6 multicast groups, a directly connected check is performed and the PIM notified if a directly connected source arrives. This procedure is how PIM sends register messages for new sources.

Examples

The following is sample output from the **show ipv6 mrib route**command using the **summary** keyword:

```
Router# show ipv6 mrib route summary
MRIB Route-DB Summary
```

```
No. of (*,G) routes = 52
No. of (S,G) routes = 0
No. of Route x Interfaces (RxI) = 10
```

The table below describes the significant fields shown in the display.

Table 100: show ipv6 mrib route Field Descriptions

Field	Description
No. of (*, G) routes	Number of shared tree routes in the MRIB.
No. of (S, G) routes	Number of source tree routes in the MRIB.
No. of Route x Interfaces (RxI)	Sum of all the interfaces on each MRIB route entry.

show ipv6 mroute

To display the information in the PIM topology table in a format similar to the **show ip mroute** command, use the **show ipv6 mroute** command in user EXEC or privileged EXEC mode.

show ipv6 mroute [**vrf** *vrf-name*] [{**link-local** | [{*group-name* | *group-address* [{*source-addresssource-name*}]}]}] [**summary**] [**count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
source-address | *source-name*	(Optional) IPv6 address or name of the source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IPv6 multicast routing table.
count	(Optional) Displays statistics from the Multicast Forwarding Information Base (MFIB) about the group and source, including number of packets, packets per second, average packet size, and bytes per second.

Command Default

The **show ipv6 mroute** command displays all groups and sources.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(25)S	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Release	Modification
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The IPv6 multicast implementation does not have a separate mroute table. For this reason, the **show ipv6 mroute** command enables you to display the information in the PIM topology table in a format similar to the **show ip mroute** command.

If you omit all optional arguments and keywords, the **show ipv6 mroute** command displays all the entries in the PIM topology table (except link-local groups where the **link-local** keyword is available).

The Cisco IOS software populates the PIM topology table by creating (S,G) and (*,G) entries based on PIM protocol messages, MLD reports, and traffic. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Use the **show ipv6 mroute**command to display the forwarding status of each IPv6 multicast route.

Examples

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

```
Router# show ipv6 mroute ff07::1
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

The following is sample output from the **show ipv6 mroute**command with the **summary**keyword:

```
Router# show ipv6 mroute ff07::1 summary
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, OIF count:1, flags:S
(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT
```

The following is sample output from the **show ipv6 mroute**command with the **count**keyword:

```
Router# show ipv6 mroute ff07::1 count
IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
```

```
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group:FF07::1
  RP-tree:
   RP Forwarding:0/0/0/0, Other:0/0/0
   LC Forwarding:0/0/0/0, Other:0/0/0
  Source:2001:0DB8:999::99,
   RP Forwarding:0/0/0/0, Other:0/0/0
   LC Forwarding:0/0/0/0, Other:0/0/0
   HW Forwd:  20000/0/92/0, Other:0/0/0
  Tot. shown:Source count:1, pkt count:20000
```

The table below describes the significant fields shown in the display.

Table 101: show ipv6 mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry. • S--sparse. Entry is operating in sparse mode. • s--SSM group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes. • C--connected. A member of the multicast group is present on the directly connected interface. • L--local. The router itself is a member of the multicast group. • I--received source specific host report. Indicates that an (S, G) entry was created by an (S, G) report. This flag is set only on the designated router (DR). • P--pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source. • R--RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source. • F--register flag. Indicates that the software is registering for a multicast source. • T--SPT-bit set. Indicates that packets have been received on the shortest path source tree. • J--join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold value set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. The default SPT-Threshold value of 0 kbps is used for the group, and the J - Join SPT flag is always set on (*, G) entries and is never cleared. The router immediately switches to the shortest path source tree when traffic from a new source is received.
Timers: Uptime/Expires	"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IPv6 multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.

Field	Description
Interface state:	Indicates the state of the incoming or outgoing interface. • Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list. • Next-Hop. "Next-Hop" specifies the IP address of the downstream neighbor. • State/Mode. "State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists. "Mode" indicates that the interface is operating in sparse mode.
(*, FF07::1) and (2001:0DB8:999::99)	Entry in the IPv6 multicast routing table. The entry consists of the IPv6 address of the source router followed by the IPv6 address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries; (*, G) entries are used to build (S, G) entries.
RP	Address of the RP router.
flags:	Information set by the MRIB clients on this MRIB entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF nbr	IP address of the upstream router to the RP or source.
Outgoing interface list:	Interfaces through which packets will be forwarded. For (S,G) entries, this list will not include the interfaces inherited from the (*,G) entry.

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib	Displays the forwarding entries and interfaces in the IPv6 MFIB.

show ipv6 mroute active

To display the active multicast streams on the router, use the **show ipv6 mroute active**command in user EXEC or privileged EXEC mode.

show **ipv6** **mroute** [**vrf** *vrf-name*] [{**link-local***group-namegroup-address*}] **active** [**kbps**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
link-local	(Optional) Displays the link-local groups.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
kbps	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at the kbps value or higher. The *kbps* argument defaults to 4 kbps.

Command Default

The *kbps* argument defaults to 4 kbps.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **link-local** keyword was added.
12.3(4)T	The **link-local** keyword was added.
12.2(25)S	The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 mroute active**command displays active multicast streams with data rates that are greater than or equal to the kilobits per second set by the user. The command default is 4 kbps.

Examples

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

```
Router# show ipv6 mroute active
Active IPv6 Multicast Sources - sending >= 4 kbps
Group:FF05::1
 Source:2001::1:1:1
   Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

The table below describes the significant fields shown in the display.

Table 102: show ipv6 mroute active Field Descriptions

Field	Description
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Rate...kbps	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.

show ipv6 mtu

To display maximum transmission unit (MTU) cache information for IPv6 interfaces, use the **show ipv6 mtu**command in user EXEC or privileged EXEC mode.

show ipv6 mtu [**vrf** *vrfname*]

Syntax Description

vrf	(Optional) Displays an IPv6 Virtual Private Network (VPN) routing/forwarding instance (VRF).
vrfname	(Optional) Name of the IPv6 VRF.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	The **vrf** keyword and *vrfname* argument were added.

Usage Guidelines

The **vrf** keyword and *vrfname* argument allow you to view MTUs related to a specific VRF.

Examples

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

```
Router# show ipv6 mtu
MTU     Since    Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
```

The following is sample output from the **show ipv6 mtu** command using the **vrf** keyword and *vrfname* argument. This example provides information about the VRF named vrfname1:

```
Router# show ipv6 mtu vrf vrfname1
MTU   Since       Source Address     Destination Address
1300  00:00:04    2001:0DB8:2        2001:0DB8:7
```

The table below describes the significant fields shown in the display.

Table 103: show ipv6 mtu Field Descriptions

Field	Description
MTU	MTU, which was contained in the Internet Control Message Protocol (ICMP) packet-too-big message, used for the path to the destination address.
Since	Age of the entry since the ICMP packet-too-big message was received.
Destination Address	Address contained in the received ICMP packet-too-big message. Packets originating from this router to this address should be no bigger than the given MTU.

Related Commands

Command	Description
ipv6 mtu	Sets the MTU size of IPv6 packets sent on an interface.

IPv6 Commands: show ipv6 na to show ipv6 pr

show ipv6 nat statistics

To display Network Address Translation--Protocol Translation (NAT-PT) statistics, use the **show iv6 nat statistics**command in user EXEC or privileged EXEC mode.

show ipv6 nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

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

```
Router# show ipv6 nat statistics
Total active translations: 4 (2 static, 2 dynamic; 2 extended)
NAT-PT interfaces:
  Ethernet3/1, Ethernet3/3
Hits: 1  Misses: 1
Expired translations: 0
```

The table below describes the significant fields shown in the display.

Table 104: show ipv6 nat statistics Field Descriptions

Field	Description
Total active translations	Number of translations active in the system. This number increments by one each time a translation is created and is decremented each time a translation is cleared or times out. Displays the numbers for each type of translation.
NAT-PT interfaces	The interfaces, by type and number, that are configured to run NAT-PT translations.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.

Related Commands

Command	Description
show ipv6 nat translations	Displays active NAT-PT translations.

show ipv6 nat translations

To display active Network Address Translation--Protocol Translation (NAT-PT) translations, use the **show ip nat translations** command in user EXEC or privileged EXEC mode.

show ipv6 nat translations [{**icmp** | **tcp** | **udp**}] [**verbose**]

Syntax Description

icmp	(Optional) Displays detailed information about NAT-PT ICMP translation events.
tcp	(Optional) Displays detailed information about NAT-PT TCP translation events.
udp	(Optional) Displays detailed information about NAT-PT User Datagram Protocol (UDP) translation events.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Two static translations have been configured between an IPv4 source address and an IPv6 destination, and vice versa.

```
Router# show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.123.2            2001::2
---   ---                      ---
      192.168.122.10           2001::10
tcp   192.168.124.8,11047      3002::8,11047
      192.168.123.2,23         2001::2,23
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,69         2001::2,69
udp   192.168.124.8,52922      3002::8,52922
      192.168.123.2,52922      2001::2,52922
---   192.168.124.8            3002::8
      192.168.123.2            2001::2
---   192.168.124.8            3002::8
      ---                      ---
---   192.168.121.4            5001::4
      ---                      ---
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ipv6 nat translations verbose
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
```

```
---   ---                     ---
      192.168.123.2           2001::2
      create 00:04:24, use 00:03:24,
---   ---                     ---
      192.168.122.10          2001::10
      create 00:04:24, use 00:04:24,
tcp   192.168.124.8,11047     3002::8,11047
      192.168.123.2,23        2001::2,23
      create 00:03:24, use 00:03:20, left 00:16:39,
udp   192.168.124.8,52922     3002::8,52922
      192.168.123.2,69        2001::2,69
      create 00:02:51, use 00:02:37, left 00:17:22,
udp   192.168.124.8,52922     3002::8,52922
      192.168.123.2,52922     2001::2,52922
      create 00:02:48, use 00:02:30, left 00:17:29,
---   192.168.124.8           3002::8
      192.168.123.2           2001::2
      create 00:03:24, use 00:02:34, left 00:17:25,
---   192.168.124.8           3002::8
      ---                     ---
      create 00:04:24, use 00:03:24,
---   192.168.121.4           5001::4
      ---                     ---
      create 00:04:25, use 00:04:25,
```

The table below describes the significant fields shown in the display.

Table 105: show ipv6 nat translations Field Descriptions

Field	Description
Prot	Protocol of the port identifying the address.
IPv4 source/IPv6 source	The IPv4 or IPv6 source address to be translated.
IPv4 destination/IPv6 destination	The IPv4 or IPv6 destination address.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
left	Time before the entry times out (in hours:minutes:seconds).

Related Commands

Command	Description
clear ipv6 nat translation	Clears dynamic NAT-PT translations from the translation state table.

show ipv6 nd destination

To display information about IPv6 host-mode destination cache entries, use the **show ipv6 nd destination** command in user EXEC or privileged EXEC mode.

show ipv6 nd destination [**vrf** *vrf-name*] [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface- type	(Optional) Specifies the Interface type.
interface- number	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **show ipv6 nd destination** command to display information about IPv6 host-mode destination cache entries. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is displayed. If the *interface-type* and *interface-number* arguments are used, then only information about the specified interface is displayed.

Examples

```
Device# show ipv6 nd destination

IPv6 ND destination cache (table: default)
Code: R - Redirect
   2001::1 [8]
    via FE80::A8BB:CCFF:FE00:5B00/Ethernet0/0
```

The following table describes the significant fields shown in the display.

Table 106: show ipv6 nd destination Field Descriptions

Field	Description
Code: R - Redirect	Destinations learned through redirect.
2001::1 [8]	The value displayed in brackets is the time, in seconds, since the destination cache entry was last used.

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

show ipv6 nd on-link prefix

To display information about on-link prefixes learned through router advertisements (RAs), use the **show ipv6 nd on-link prefix** command in user EXEC or privileged EXEC mode.

show ipv6 nd on-link prefix [**vrf** *vrf-name*] [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface -type	(Optional) Specifies the Interface type.
interface -number	(Optional) Specifies the Interface number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **show ipv6 nd on-link prefix** command to display information about on-link prefixes learned through RAs.

Prefixes learned from an RA may be inspected using the **show ipv6 nd on-link prefix** command. If the **vrf** *vrf-name* keyword and argument pair is used, then only information about the specified VRF is displayed. If the *interface-type* and *interface-number* arguments are used, then only information about the specified interface is displayed.

Examples

The following example displays information about on-link prefixes learned through RAs:

```
Device# show ipv6 nd on-link prefix

IPv6 ND on-link Prefix (table: default), 2 prefixes
Code: A - Autonomous Address Config
A  2001::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
2001:1:2::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
```

Related Commands

Command	Description
ipv6 nd host mode strict	Enables the conformant, or strict, IPv6 host mode.

show ipv6 nd raguard counters

To display information about RA guard counters, use the **show ipv6 nd raguard policy**command in privileged EXEC mode.

show ipv6 nd raguard counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(5th)SXI	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard counters** command displays information about RA guard counters, such as packets sent, packets received, and packets droped. This command also provides information on why a packet was dropped.

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [*policy-name*]

Syntax Description

policy-name	(Optional) RA guard policy name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 nd raguard policy** command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

The following example shows the policy configuration for a policy named raguard1 and all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

The table below describes the significant fields shown in the display.

Table 107: show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which the RA guard feature is configured.

show ipv6 nd secured certificates

To display active IPv6 Secure Neighbor Discovery (SeND) certificates, use the **show ipv6 nd secured certificates**command in privileged EXEC mode.

show ipv6 nd secured certificates

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND certificates are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured certificates** command is used on hosts (routers configured in host mode) to display the certifcates received over SeND (via Certificate Path Advertisement) and their state.

Examples

The following example displays active SeND certificates:

```
Router# show ipv6 nd secured certificates
Total number of entries: 1 / 32
Hash                             id         RA  certcnt certrcv state
DC0102E09FAF422D49ED79A846D2EBC1 0x00000778 no  1       1       CERT_VALIDATED
certificate No 0
subject  hostname=sa14-72a,c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=72a
```

issuer c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=CA0

The table below describes the significant fields shown in the display.

Table 108: show ipv6 nd secured certificates Field Descriptions

Field	Description
certcnt	Number of certificate for this chain.
certrcv	Number of certifciate received in the chain.
Hash	Key hash.
id	Numero of the certifciate.
RA	Displays Yes if an RA is pending for this certifciate.
state	Current state of the certificate.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 nd secured counters interface

To display IPv6 Secure Neighbor Discovery (SeND) counters on an interface, use the **show ipv6 nd secured counters interface**command in privileged EXEC mode.

show ipv6 nd secured counters interface *interface*

Syntax Description

interface	(Optional) Specifies the interface on which SeND counters are located.

Command Default

No SeND counter information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays SeND counters:

```
Router# show ipv6 nd secured counters interface ethernet0/0
e0/0 Received ND messages on Ethernet0/0:
rcvd    accept  SLLA    TLLA    PREFIX  MTU     CGA     RSA     TS      NONCE   TA CERT
RA      66      65      63      0       62      63      63      63      63      0       0
      0
NS      8       8       8       0       0       0       8       8       8       8       0
      0
NA      20      20      0       8       0       0       19      19      19      14      0
      0
CPA     1       1       0       0       0       0       0       0       0       0       1
      1
Dropped ND messages on Ethernet0/0:
Codes   TIMEOUT: Timed out while waiting for rsp
        drop    TIMEOUT
RA      1       1
Sent ND messages on Ethernet0/0:
sent    aborted SLLA    CGA     RSA     TS      NONCE   TA
NS      14      0       14      14      14      14      14      0
NA      8       0       0       8       8       8       8       0
CPS     43      0       0       0       0       0       0       43
Router#
```

The table below describes the significant fields shown in the display.

Table 109: show ipv6 nd secured counters interface Field Descriptions

Field	Description
accept	Number of neighbor discovery (ND) messages accepted (messages that are not dropped).
CERT	Number of messages received with the certificate option.
CGA	Number of messages received with the CGA option.

Field	Description
MTU	Number of messages received with the MTU option.
NA	Number of NDP neighbor advertisements
NONCE	Number of messages received with the NONCE option.
NS	Number of NDP neighbor solicitions.
PREFIX	Number of messages received with the PREFIX option.
rcvd	Number of ND messages received on the interface.
RA	Number of router advertisements.
REDIR	Number of NDP redirect messages.
RS	Router Solicit.
RSA	Number of messages received with the RSA option.
SLLA	Number of messages received with the ND SLLA option.
TA	Number of messages received with the trust anchor option.
TS	Number of messages received with the time stamp option.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND timestamp entries.

show ipv6 nd secured nonce-db

To display active IPv6 Secure Neighbor Discovery (SeND) nonce database entries, use the **show ipv6 nd secured nonce-db**command in privileged EXEC mode.

show ipv6 nd secured nonce-db

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND nonce information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured nonce-db**command is used to display the pending solicitations. There are rarely any pending solicitations because the solicitations are quickly answered and removed from the database.

Examples

The following example displays active SeND nonce entries. The output is self-explanatory.

```
Router# show ipv6 nd secured nonce-db
Total number of entries: 0
```

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured timestamp-db	Displays active SeND time stamp entries.

show ipv6 nd secured solicit-db

To display pending SEcure Neighbor Discovery (SEND) solicitations from peers, use the **show ipv6 nd secured solicit-db**command in privileged EXEC configuration mode.

show ipv6 nd secured solicit-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SEND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to display pending SEND solicitations.

Examples

The following example displays pending SEcure Neighbor Discovery (SEND) solicitations from peers:

```
Router# show ipv6 nd secured solicit-db
```

show ipv6 nd secured timestamp-db

To display active Secure Neighbor Discovery (SeND) time-stamp database entries, use the **show ipv6 nd secured timestamp-db**command in privileged EXEC mode.

show ipv6 nd secured timestamp-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SeND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured timestamp-db** command displays the content of the time-stamp databse, which contains last received messages from peers. It also displays the delta and fuzz values.

Examples

The following example displays active SeND time-stamp database entries:

```
Router# show ipv6 nd secured timestamp-db
Total number of entries: 6 Number of unreached peer entries: 3 / 1024
FE80::289C:3308:4719:87F2 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 41m 16s (reached)
        TSlast: 0x4936B97655FF = Wed Dec  3 16:53:10 2008
        RDlast: 0x4936B976438B = Wed Dec  3 16:53:10 2008
FE80::2441:88D1:22FC:3B77 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 59m 53s (reached)
        TSlast: 0x4936BDD2E13E = Wed Dec  3 17:11:46 2008
        RDlast: 0x4936BDD2D0D6 = Wed Dec  3 17:11:46 2008
FE80::E2:F012:6F72:9E45 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 18s (unreached)
        TSlast: 0x4936B0CBB333 = Wed Dec  3 16:16:11 2008
        RDlast: 0x4936B0CBBD70 = Wed Dec  3 16:16:11 2008 2001:100::38C9:4A1A:2972:794E on
 Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 19s (unreached)
        TSlast: 0x4936BA254FDA = Wed Dec  3 16:56:05 2008
        RDlast: 0x4936BA253F72 = Wed Dec  3 16:56:05 2008 2001:100::383E:6BD5:397:4A50 on
Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 45m 0s (reached)
        TSlast: 0x4936BA55F2AA = Wed Dec  3 16:56:53 2008
        RDlast: 0x4936BA55E036 = Wed Dec  3 16:56:53 2008
2001:100::434:E62D:327D:B1E6 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 42s (unreached)
        TSlast: 0x4936B0E422D0 = Wed Dec  3 16:16:36 2008
        RDlast: 0x4936B0E42D0E = Wed Dec  3 16:16:36 2008
```

The table below describes the significant fields shown in the display.

Table 110: show ipv6 nd secured timestamp-db Field Descriptions

Field	Description
Total number of entries	Number of entries (peers) in the cache.
Time to expire	Remaining time before entry expires.
TSlast	Last peer timestamp value.
RDlast	Time when the last message was received from the peer.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.

show ipv6 neighbor binding

To display contents of a binding table, use the **show ipv6 neighbor binding** command in privileged EXEC mode.

show ipv6 neighbor binding [{**vlan** *vlan-id* | **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*}]

Syntax Description

vlan *vlan-id*	(Optional) Displays the binding table entries that match the specified VLAN.
interface *type number*	(Optional) Displays the binding table entries that match the specified interface type and number.
ipv6 *ipv6-address*	(Optional) Displays the binding table entries that match the specified IPv6 address.
mac *mac-address*	(Optional) Displays the binding table entries that match the specified Media Access Control (MAC) address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE.	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 neighbor binding** command displays the contents of the binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all binding table contents are displayed.

The following keyword and argument combinations are allowed:

- **vlan** *vlan-id*: Displays all entries for the specified VLAN.
- **interface** *type number*: Displays all entries for the specified interface.
- **ipv6** *ipv6-address* + **interface** *type number* + **vlan** *vlan-id*: Displays a single entry that matches these three keyword and argument combinations.
- **ipv6** *ipv6-address* + **interface** *type number*: Displays all entries for the specified IPv6 address and interface.
- **ipv6** *ipv6-address*: Displays all entries for the specified IPv6 address.

Examples

The following example displays the contents of a binding table:

```
Device# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
    IPv6 address            Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0 REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203 DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0 REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0 REACHABLE  9559
ND  2001:100::2                AABB.CC01.F600  Et1/0     200  0002    0 REACHABLE  9196
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188 DOWN       N/A
S   2001:500::1                000A.000B.000C  Fa4/13    300  0080 8676 STALE      N/A
```

The table below describes the significant fields shown in the display.

Table 111: show ipv6 neighbor binding Field Descriptions

Field	Description
address DB has *n* entries	Number of entries in the specified database.

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

show ipv6 neighbors

To display IPv6 neighbor discovery (ND) cache information, use the **show ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 neighbors [{*interface-type interface-numberipv6-addressipv6-hostname* | **statistics**}]

Syntax Description

interface-type	(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.
interface-number	(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.
ipv6-address	(Optional) Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-hostname	(Optional) Specifies the IPv6 hostname of the remote networking device.
statistics	(Optional) Displays ND cache statistics.

Command Default

All IPv6 ND cache entries are listed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. Support for static entries in the IPv6 neighbor discovery cache was added to the command output.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and introduced on Cisco ASR 1000 Series devices.

Release	Modification
Cisco IOS XE Release 2.6	This command was modified. This command was updated to display the number and the limit of ND cache entries on a particular interface.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

Specifying the **statistics** keyword displays ND cache statistics.

The following is sample output from the **show ipv6 neighbors** command when entered with an interface type and number:

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH Ethernet2
3001:1::45a                                 - 0002.7d1a.9472  REACH Ethernet2
```

The following is sample output from the **show ipv6 neighbors** command when entered with an IPv6 address:

```
Device# 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 Ethernet2
```

The table below describes the significant fields shown in the displays.

Table 112: show ipv6 neighbors Field Descriptions

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

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

The following is sample output from the **show ipv6 neighbors** command with the **statistics** keyword:

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
 Entries 2, High-water 2, Gleaned 1, Scavenged 0
 Entry States
   INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
 Resolutions (INCMP)
   Requested 1, timeouts 0, resolved 1, failed 0
   In-progress 0, High-water 1, Throttled 0, Data discards 0
 Resolutions (PROBE)
   Requested 3, timeouts 0, resolved 3, failed 0
```

The table below describes the significant fields shown in this display:

Table 113: show ipv6 neighbors statistics Field Descriptions

Field	Description
Entries	Total number of ND neighbor entries in the ND cache.
High-Water	Maximum amount (so far) of ND neighbor entries in ND cache.
Gleaned	Number of ND neighbor entries gleaned (that is, learned from a neighbor NA or other ND packet).
Scavenged	Number of stale ND neighbor entries that have timed out and been removed from the cache.
Entry States	Number of ND neighbor entries in each state.
Resolutions (INCMP)	Statistics for neighbor resolutions attempted in INCMP state (that is, resolutions prompted by a data packet). Details about the resolutions attempted in INCMP state are follows: • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions. • In-progress--Number of resolutions in progress. • High-water--Maximum number (so far) of resolutions in progress. • Throttled--Number of times resolution request was ignored due to maximum number of resolutions in progress limit. • Data discards--Number of data packets discarded that are awaiting neighbor resolution.
Resolutions (PROBE)	Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet): • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions.

show ipv6 nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ipv6 nhrp** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp [{**dynamic** [*ipv6-address*] | **incomplete** | **static**}] [{**address** | **interface**}] [{**brief** | **detail**}] [**purge**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IPv6-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
ipv6-address	(Optional) The IPv6 address of the cache entry.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IPv6-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
static	(Optional) Displays static IPv6-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ipv6 nhrp map** command. See the table below for types, number ranges, and descriptions.
address	(Optional) NHRP mapping entry for specified protocol addresses.
interface	(Optional) NHRP mapping entry for the specified interface. See the table below for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 114: Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

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

```
Router# show ipv6 nhrp
2001:0db8:3c4d:0015::1a2f:3d2c/48  via
2001:0db8:3c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

The table below describes the significant fields shown in the display.

Table 115: show ipv6 nhrp Field Descriptions

Field	Description
2001:0db8:3c4d:0015::1a2f: 3d2c/48	Target network.
2001:0db8:3c4d:0015::1a2f:3d2c	Next hop to reach the target network.
Tunnel0	Interface through which the target network is reached.
created 6d05h	Length of time since the entry was created (dayshours).
never expire	Indicates that static entries never expire.

The following is sample output from the **show ipv6 nhrp**command using the **brief** keyword:

```
Router# show ipv6 nhrp brief
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48
 via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99
```

The table below describes the significant fields shown in the display.

Table 116: show ipv6 nhrp brief Field Descriptions

Field	Description
2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c/48	Target network.
via 2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c	Next Hop to reach the target network.
Interface: Tunnel0	Interface through which the target network is reached.
Type: static	Type of tunnel. The types can be one of the following: • dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static--NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static. • incomplete--The NBMA address is not known for the target network.

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.

show ipv6 nhrp multicast

To display Next Hop Resolution Protocol (NHRP) multicast mapping information, use the **show ipv6 nhrp multicast**command in user EXEC or privileged EXEC mode.

show ipv6 nhrp multicast [{**ipv4-address** | **interface***ipv6-address*}]

Syntax Description

ipv4-address	(Optional) The IPv4 address of the multicast mapping entry.
interface	(Optional) All multicast mapping entries of the NHRP network for the interface. See the table below for interface types, number ranges, and descriptions.
ipv6-address	(Optional) The IPv6 address of the multicast mapping entry.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.2(1)T	This command was modified. The *ipv4-address* argument was added.

Usage Guidelines

The table below lists valid interface types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 117: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex

Valid Types	Number Ranges	Interface Descriptions
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ipv6 nhrp multicast** command. Fields in the display are self-explanatory.

```
Router# show ipv6 nhrp multicast
  I/F     NBMA address
Tunnel1    192.169.2.10    Flags: dynamic
Tunnel1    192.169.2.11    Flags: dynamic
```

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.

show ipv6 nhrp multicast stats

To display multicast mapping statistics for one or all interfaces, use the **show ipv6 nhrp multicast stats** command in Privileged EXEC mode. The command displays statistics such as the count of enqueued, dequeued, and dropped packets.

show ipv6 nhrp multicast [*interface-name*] **stats**

Syntax Description

interface-name	Displays multicast mapping statistics for the specified interface. Example: **`show ipv6 nhrp multicast tunnel0 stats`**

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.8.1	Command introduced.

Example

```
SPOKE1#show ipv6 nhrp multicast stats
Legend: (m/n) - (m packets/n milliseconds)
============================================================================================

Global stats
Total multicast pkts enqueued     4
Total multicast failed to enqueue 0
Total multicast pkts dequeued     4
Invalid multicast pkts dequeued   0
Total multicast pkts dropped      0

Interface stats
                                  Enqueued/Failed            Dequeued/Rep fail      Dropped
                           --------------------------  --------------------------  ----------
 Tu0     (250    /     10)              4/0                         4/0                    0
```

show ipv6 nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ipv6 nhrp nhs** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp nhs [*interface-type interface-number*] [{**detail** | **redundancy**}] [{**cluster** *number* | **preempted** | **running** | **waiting**}]

Syntax Description

interface-type	(Optional) Type of interface for which NHS information should be displayed. See the table below for types, number ranges, and descriptions.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed NHS information.
redundancy	(Optional) Displays NHS recovery information.
cluster *number*	(Optional) Displays NHS recovery cluster information. The range is from 0 to 10.
preempted	(Optional) Displays NHSs that come up and are preempted.
running	(Optional) Displays NHSs that are responding or expecting replies.
waiting	(Optional) Displays NHSs that are waiting to be scheduled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.1(2)T	This command was modified. The **redundancy**, **cluster** *number*, **preempted**, **running**, and **waiting** keywords and argument were added.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface-interface*argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 118: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async

Valid Types	Number Ranges	Interface Descriptions
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	Fast Ethernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

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

```
Router# show ipv6 nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
192.0.2.1  W priority = 2 cluster = 0
192.0.2.2  RE priority = 0 cluster = 0
192.0.2.3  RE priority = 1 cluster = 0
```

The following is sample output from the **show ipv6 nhrp nhs redundancy** command:

```
Router# show ipv6 nhrp nhs redundancy
Legend: E=Expecting replies, R=Responding, W=Waiting
No.  Interface  Cluster  NHS         Priority  Cur-State  Cur-Queue  Prev-State Prev-Queue
1    Tunnel0    5        2001::101   1         E          Running     RE        Running
```

```
No.  Interface  Cluster  Status  Max-Con  Total-NHS Responding Expecting Waiting Fallback
1    Tunnel0    5        Disable Not Set  1         0          1         0       0
```

The table below describes the significant field shown in the display.

Table 119: show ipv6 nhrp nhs Field Descriptions

Field	Description
Tunnel0	Interface through which the target network is reached.
priority	Priority value assigned to the NHS.
cluster	Group to which the NHS belong.
E=Expecting replies	NHSs that are active and expecting replies.
R=Responding	NHSs that are active and responding.
W=Waiting	NHSs that are preempted and are not in the active probe list.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.

show ipv6 nhrp summary

To display Next Hop Resolution Protocol (NHRP) mapping summary information, use the **show ipv6 nhrp summary**command in user EXEC or privileged EXEC mode.

show ipv6 nhrp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use this command to monitor NHRP.

Examples

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

```
Router# show ipv6 nhrp summary
IPV6 NHRP cache 1 entry, 256 bytes
    1 static  0 dynamic  0 incomplete
```

The table below describes the significant field shown in the display.

Table 120: show ipv6 nhrp summary Field Descriptions

Field Output	Description
static	NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static.
dynamic	NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations
incomplete	The nonbroadcast multiaccess (NBMA) address is not known for the target network.

Related Commands

Command	Description
ip nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ipv6 nhrp	Displays NHRP mapping information.

show ipv6 nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ipv6 nhrp traffic** command in privileged EXEC mode.

show ipv6 nhrp traffic [{**throttled** | **interface**{**tunnel** *number* | **Virtual-Access** *number*}}]

Syntax Description

throttled	(Optional) Displays information about NHRP traffic that is throttled.
interface	(Optional) Displays NHRP traffic information for a given interface.
tunnel *number*	(Optional) Specifies the tunnel interface number.
Virtual-Access *number*	Specifies the virtual access interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.3(2)T	This command was modified. The **Virtual-Access** *number* keyword-argument pair was added.
Cisco IOS XE 16.3.2	This command was modified. The **throttled** keyword was added.

Usage Guidelines

Use this command to monitor NHRP traffic information.

Examples

The following example provides output for IPv6 NHRP traffic statistics:

```
Router# show ipv6 nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 8
1 Resolution Request 1 Resolution Reply 6 Registration Request
0 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 0 Traffic Indication
Rcvd: Total 5
1 Resolution Request 1 Resolution Reply 0 Registration Request
2 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 1 Traffic Indication
```

The table below describes the significant field shown in the display.

Table 121: show ipv6 nhrp traffic Field Descriptions

Field Output	Description
tunnel0:	Displays information about a specified tunnel; in thhis case, Tunnel0.

Field Output	Description
Max-send limit: 100Pkts/10Sec, Usage: 0%	The maximum number of packets allowed to be sent in a specified time, and the current usage.
Sent: Total 8	Number of packets sent.
1 Resolution Request 1 Resolution Reply 6 Registration Request 0 Registration Reply 0 Purge Request 0 Purge Reply	Description and breakdown of of the types of packets sent.
0 Error Indication 0 Traffic Indication	Number of errors in the sent packets.
Rcvd: Total 5	Number of packets received.
1 Resolution Request 1 Resolution Reply 0 Registration Request 2 Registration Reply 0 Purge Request 0 Purge Reply	Description and breakdown of the types of packets received.
0 Error Indication 1 Traffic Indication	Number of errors in the sent packets.

show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] [**rate-limit**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Area ID. This argument displays information about a specified area only.
rate-limit	(Optional) Rate-limited link-state advertisements (LSAs). This keyword displays LSAs that are currently being rate limited, together with the remaining time to the next generation.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.4(15)XF	Command output was modified to include VMI PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The **rate-limit** keyword was added. Command output was modified to include the configuration values for SPF and LSA throttling timers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.

Release	Modification
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Examples

show ipv6 ospf Output Example

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

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this device is 1. 1 normal 0 stub 0 nssa
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        MD5 Authentication, SPI 1000
        SPF algorithm executed 2 times
        Number of LSA 5. Checksum Sum 0x02A005
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The table below describes the significant fields shown in the display.

Table 122: show ipv6 ospf Field Descriptions

Field	Description
Routing process "ospfv3 1" with ID 10.10.10.1	Process ID and OSPF device ID.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of areas	Number of areas in device, area addresses, and so on.

show ipv6 ospf With Area Encryption Example

The following sample output shows the **show ipv6 ospf** command with area encryption information:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this device is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 3 times
        Number of LSA 31. Checksum Sum 0x107493
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 20
        Flood list length 0
    Area 1
        Number of interfaces in this area is 2
        NULL Encryption SHA-1 Auth, SPI 1001
        SPF algorithm executed 7 times
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The table below describes the significant fields shown in the display.

Table 123: show ipv6 ospf with Area Encryption Information Field Descriptions

Field	Description
Area 1	Subsequent fields describe area 1.
NULL Encryption SHA-1 Auth, SPI 1001	Displays the encryption algorithm (in this case, null, meaning no encryption algorithm is used), the authentication algorithm (SHA-1), and the security policy index (SPI) value (1001).

The following example displays the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary device
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

The table below describes the significant fields shown in the display.

Table 124: show ipv6 ospf with SPF and LSA Throttling Timer Field Descriptions

Field	Description
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum hold time between two consecutive SPFs	Minimum hold time between consecutive SPF calculations.
Maximum wait time between two consecutive SPFs 10000 msecs	Maximum hold time between consecutive SPF calculations.
Minimum LSA interval 5 secs	Minimum time interval (in seconds) between link-state advertisements.
Minimum LSA arrival 1000 msecs	Maximum arrival time (in milliseconds) of link-state advertisements.

The following example shows information about LSAs that are currently being rate limited:

```
Device# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
```

The table below describes the significant fields shown in the display.

Table 125: show ipv6 ospf rate-limit Field Descriptions

Field	Description
LSAID	Link-state ID of the LSA.
Type	Description of the LSA.
Adv Rtr	ID of the advertising device.
Due in:	Remaining time until the generation of the next event.

show ipv6 ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ipv6 ospf border-routers** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*] **border-routers**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
Router# show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

The table below describes the significant fields shown in the display.

Table 126: show ipv6 ospf border-routers Field Descriptions

Field	Description
i - Intra-area route, I - Inter-area route	The type of this route.
172.16.4.4, 172.16.3.3	Router ID of the destination router.
[2], [1]	Metric used to reach the destination router.

Field	Description
FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808	Link-local routers.
FastEthernet0/0, POS4/0	The interface on which the IPv6 OSPF protocol is configured.
ABR	Area border router.
ASBR	Autonomous system boundary router.
Area 0, Area 1	The area ID of the area from which this route is learned.
SPF 13, SPF 8, SPF 3	The internal number of the shortest path first (SPF) calculation that installs this route.

show ipv6 ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ipv6 ospf database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

show ipv6 ospf [*process-id* [*area-id*]] **database** [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [**database-summary**]
{**show ipv6 ospf** [*process-id* [*area-id*]] **database** [**external** [**ipv6-prefix**] [*link-state-id*]] | [{**adv-router** *router-id* | **self-originate**}] [**internal**]}
show ipv6 ospf [*process-id* [*area-id*]] **database** [**grace**]
{**show ipv6 ospf** [*process-id* [*area-id*]] **database** [**inter-area prefix** [**ipv6-prefix**] [*link-state-id*]] | [{**adv-router** *router-id* | **self-originate**}] [**internal**]}
{**show ipv6 ospf** [*process-id* [*area-id*]] **database** [**inter-area router** [**destination-router-id**] [*link-state-id*]] | [{**adv-router** *router-id* | **self-originate**}] [**internal**]}
show ipv6 ospf [*process-id* [*area-id*]] **database** [**link** [**interface** *interface-name*] [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [**network** [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [**nssa-external** [*ipv6-prefix*] [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [**prefix** [**ref-lsa** {**router** | **network**}] [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [**router** [*link-state-id*]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [{[{**router** | **network** | [{**external** *ipv6-prefix* | **nssa-external** *ipv6-prefix* | **inter-area** {**prefix** *ipv6-prefix* | **router**}}] | **link** | **prefix**}] | **database-summary**}] [{**adv-router** *router-id* | **self-originate**}] [**internal**]
show ipv6 ospf [*process-id* [*area-id*]] **database** [**unknown** [{**area** | **as** | **link**} [*link-state-id*]]] [{**adv-router** *router-id* | **self-originate**}] [**internal**]

Syntax Description

process-id	(Optional) Displays information only about a specified process.
area-id	(Optional) Displays information only about a specified area. The *area-id* argument can only be used if the *process-id* argument is specified.
adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
internal	(Optional) Internal LSA information.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
external	(Optional) Displays information only about the external LSAs.

ipv6-prefix	(Optional) Link-local IPv6 address of the neighbor. 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-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
destination-router-id	(Optional) The specified destination router ID.
link	(Optional) Displays information about the link LSAs.
interface	(Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information on the intra-area-prefix LSAs.
ref-lsa {**router** | **network**	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays all LSAs with unknown types.
area	(Optional) Filters unknown area LSAs.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
link	(Optional) When following the **unknown** keyword, the **link** keyword filters link-scope LSAs.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	The **grace** keyword was added to show information about OSPFv3 graceful restart.

Usage Guidelines

The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf** database command to provide more detailed information.

Examples

The following is sample output from the **show ipv6 ospf database** command when no arguments or keywords are used:

```
Router# show ipv6 ospf database
            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)
                Router Link States (Area 0)
ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Router Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
            Intra Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

The table below describes the significant fields shown in the display.

Table 127: show ipv6 ospf database Field Descriptions

Field	Description
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Link ID	Interface ID number.

Field	Description
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

The following is sample output from the **show ipv6 ospf database** command with the **router self-originate** keywords:

```
Router# show ipv6 ospf database router self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Router Link States (Area 0)
  LS age: 383
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000003
  Checksum: 0x7543
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: another Router (point-to-point)
      Link Metric: 1
      Local Interface ID: 14
      Neighbor Interface ID: 14
      Neighbor Router ID: 172.16.4.4
```

The following is sample output from the **show ipv6 ospf database** command with the **network**keyword:

```
Router# show ipv6 ospf database network

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Net Link States (Area 1)
  LS age: 419
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Network Links
  Link State ID: 3 (Interface ID of Designated Router)
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x8148
  Length: 32
        Attached Router: 172.16.6.6
        Attached Router: 172.16.3.3
```

The following is sample output from the **show ipv6 ospf database** command with the **link self-originate**keywords:

```
Router# show ipv6 ospf database link self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Link (Type-8) Link States (Area 0)
  LS age: 505
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Link-LSA (Interface: POS4/0)
  Link State ID: 14 (Interface ID)
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000002
```

```
  Checksum: 0xABF6
  Length: 60
  Router Priority: 1
  Link Local Address: FE80::205:5FFF:FED3:6408
  Number of Prefixes: 2
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None
```

The following is sample output from the **show ipv6 ospf database** command with the **prefix self-originate**keywords:

```
Router# show ipv6 ospf database prefix self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Intra Area Prefix Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 552
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000002
  Checksum: 0xA910
  Length: 48
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.6.6
  Number of Prefixes: 2
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None, Metric: 1
  Prefix Address: FEC0:4466::
  Prefix Length: 32, Options: None, Metric: 1
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area prefix self-originate**keywords:

```
Router# show ipv6 ospf database inter-area prefix self-originate

            OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
            Inter Area Prefix Link States (Area 0)
  LS age: 587
  LS Type: Inter Area Prefix Links
  Link State ID: 0
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x1395
  Length: 32
  Metric: 1
  Prefix Address: FEC0:3366::
  Prefix Length: 32, Options: None
  LS age: 532
  LS Type: Inter Area Prefix Links
  Link State ID: 1
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x3197
  Length: 32
  Metric: 2
  Prefix Address: FEC0:3344::
  Prefix Length: 32, Options: None
  LS age: 422
  LS Type: Inter Area Prefix Links
```

```
  Link State ID: 2
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0xCB74
  Length: 32
  Metric: 1
  Prefix Address: FEC0::
  Prefix Length: 32, Options: None
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area router self-originate**keywords:

```
Router# show ipv6 ospf database inter-area router self-originate

           OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
           Inter Area Router Link States (Area 0)
  LS age: 578
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Inter Area Router Links
  Link State ID: 50529027
  Advertising Router: 172.16.6.6
  LS Seq Number: 80000001
  Checksum: 0x369F
  Length: 32
  Metric: 1
  Destination Router ID: 172.16.3.3
```

The following is sample output from the **show ipv6 ospf database** command with the **external**keyword:

```
Router# show ipv6 ospf database external
           OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
           Type-5 AS External Link States
  Routing Bit Set on this LSA
  LS age: 654
  LS Type: AS External Link
  Link State ID: 0
  Advertising Router: 172.16.3.3
  LS Seq Number: 80000001
  Checksum: 0x218D
  Length: 32
  Prefix Address: FEC0:3333::
  Prefix Length: 32, Options: None
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
```

The following is sample output from the **show ipv6 ospf database** command for a graceful-restart-capable router:

```
Router# show ipv6 ospf 1 database
            OSPFv3 Router with ID (10.2.2.2) (Process ID 1)
            Router Link States (Area 0)
ADV Router      Age         Seq#             Fragment ID  Link count  Bits
10.1.1.1         1949       0x8000000e          0            1        None
10.2.2.2         2007       0x80000011          0            1        None
            Link (Type-8) Link States (Area 0)
ADV Router      Age         Seq#              Link ID    Interface
10.1.1.1         180         0x80000006         1          PO0/2/0/0
10.2.2.2        2007         0x80000006         1          PO0/2/0/0
            Intra Area Prefix Link States (Area 0)
ADV Router      Age         Seq#              Link ID    Ref-lstype  Ref-LSID
10.1.1.1        180         0x80000006          0        0x2001          0
```

```
10.2.2.2        2007        0x80000006          0        0x2001          0
            Grace (Type-11) Link States (Area 0)
ADV Router      Age         Seq#                Link ID    Interface
10.2.2.2        2007        0x80000005            1        PO0/2/0/0
```

The following is sample outpet from the **show ipv6 ospf database** command with the **grace** keyword:

```
Router# show ipv6 ospf database grace

OSPFv3 Router with ID (10.3.33.3) (Process ID 1)
Grace (Type-11) Link States (Area 0)
  LS age: 2
  LS Type: Grace Links (Interface: Ethernet0/0)
  Link State ID: 3 (Interface ID)
  Advertising Router: 10.2.2.2
  LS Seq Number: 80000001
  Checksum: 0xE3DD
  Length: 36
  Grace Period : 120
        Graceful Restart Reason : Software reload/upgrade
```

The table below describes the significant fields shown in the display.

Table 128: show ipv6 ospf database Field Descriptions

Field	Description
Grace (Type-11)	Type 11 indicates that this router is graceful-restart capable.
LS Type: Grace Links (Interfece: Ethernet 0/0)	The link state type and interface used.
Grace Period : 120	The graceful-restart interval, in seconds.
Graceful Restart Reason: Software reload/upgrade	The reason graceful restart was activated .

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPFv3 routing processes.
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf event

To display detailed information about IPv6 Open Shortest Path First (OSPF) events, use the **show ipv6 ospf event**command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **event** [{**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**}]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
generic	(Optional) Generic information regarding OSPF for IPv6 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse-from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

An OSPF event log is kept for every OSPF instance. If you enter no keywords with the **show ipv6 ospf event** command, all information in the OSPF event log is displayed. Use the keywords to filter specific information.

Examples

The following example shows scheduling and SPF run events, LSA arrival and LSA generation events, in order from the oldest events to the latest generated events:

```
Router# show ipv6 ospf event spf lsa reverse

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
1 *Sep 29 11:59:18.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
```

```
Seq# 80007699, Age 3600
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
9 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
80007699, Age 2
10 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
11 *Sep 29 11:59:18.867: Starting SPF
12 *Sep 29 11:59:18.867: Starting Intra-Area SPF in Area 0
16 *Sep 29 11:59:18.867: Starting Inter-Area SPF in area 0
17 *Sep 29 11:59:18.867: Starting External processing
18 *Sep 29 11:59:18.867: Starting External processing in area 0
19 *Sep 29 11:59:18.867: Starting External processing in area 1
20 *Sep 29 11:59:18.867: End of SPF
21 *Sep 29 11:59:19.367: Generate Changed Type-0x2003 LSA, LSID 10.0.0.4, Seq# 80000002,
Age 3600, Area 1, Prefix 3000:11:22::/64
23 *Sep 29 11:59:20.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
24 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
25 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
26 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
27 *Sep 29 11:59:20.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
Seq# 8000769A, Age 2
28 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
29 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1, Seq#
 8000769A, Age 2
30 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
31 *Sep 29 11:59:20.867: Starting SPF
32 *Sep 29 11:59:20.867: Starting Intra-Area SPF in Area 0
36 *Sep 29 11:59:20.867: Starting Inter-Area SPF in area 0
37 *Sep 29 11:59:20.867: Starting External processing
38 *Sep 29 11:59:20.867: Starting External processing in area 0
39 *Sep 29 11:59:20.867: Starting External processing in area 1
40 *Sep 29 11:59:20.867: End of SPF
```

The table below describes the significant fields shown in the display.

Table 129: show ip ospf Field Descriptions

Field	Description
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)	Process ID and OSPF router ID.
Rcv Changed Type-0x2009 LSA	Description of newly arrived LSA.
LSID	Link-state ID of the LSA.
Adv-Rtr	ID of the advertising router.
Seq#	Link state sequence number (detects old or duplicate link state advertisements).
Age	Link state age (in seconds).
Schedule SPF	Enables SPF to run.

Field	Description
Area	OSPF area ID.
Change in LSID	Changed link-state ID of the LSA.
LSA type	LSA type.

show ipv6 ospf flood-list

To display a list of Open Shortest Path First (OSPF) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **s how ipv6 ospf flood-list**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **flood-list** *interface-type interface-number*

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to display OSPF packet pacing.

Examples

The following is sample output from the **show ipv6 ospf flood-list** command:

```
Router# show ipv6 ospf flood-list
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971
 Interface FastEthernet0/0, Queue length 0
 Interface ATM3/0, Queue length 0
```

The table below describes the significant fields shown in the display.

Table 130: show ipv6 ospf flood-list Field Descriptions

Field	Description
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)	Identification of the router for which information is displayed.
Interface POS4/0	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf graceful-restart

To display Open Shortest Path First for IPv6 (OSPFv3) graceful restart information, use the **show ipv6 ospf graceful-restart** command in privileged EXEC mode.

show ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **show ipv6 ospf graceful-restart** command to discover information about the OSPFv3 graceful restart feature.

Examples

The following example displays OSPFv3 graceful restart information:

```
Router# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

The table below describes the significant fields shown in the display.

Table 131: show ipv6 ospf graceful-restart Field Descriptions

Field	Description
Routing Process "ospf 1"	The OSPFv3 routing process ID.
Graceful Restart enabled	The graceful restart feature is enabled on this router.
restart-interval limit: 120 sec	The restart-interval limit.

Field	Description
last restart 00:00:15 ago (took 36 secs)	How long ago the last graceful restart occurred, and how long it took to occur.
Graceful Restart helper support enabled	Graceful restart helper mode is enabled. Because graceful restart mode is also enabled on this router, you can identify this router as being graceful-restart capable. A router that is graceful-restart-aware cannot be configured in graceful-restart mode.
Router status : Active	This router is in active, as opposed to standby, mode.
Router is running in SSO mode	The router is in stateful switchover mode.
OSPF restart state : NO_RESTART	The current OSPFv3 restart state.
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0	The IPv6 addresses of the current router and the checkpoint router.

Related Commands

Command	Description
show ipv6 ospf interface	Displays OSPFv3-related interface information.

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **showipv6ospfinterface** command in user EXEC or privileged mode.

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information about a specified area only.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output is changed when encryption is enabled.
12.2(33)SRB	The **brief** keyword was added.
12.4(15)XF	Output displays were modified so that VMI PPPoE interface-based local state values are displayed in the command output when a VMI interface is specified.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output was updated to display graceful restart information.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Release	Modification
15.1(1)SY	This command was was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Examples

show ipv6 ospf interface Standard Output Example

The following is sample output from the **showipv6ospfinterface** command:

```
Router# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

The table below describes the significant fields shown in the display.

Table 132: show ipv6 ospf interface Field Descriptions

Field	Description
ATM3/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type POINT_TO_POINT, Cost: 1	Network type and link-state cost.

Field	Description
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Cisco IOS Release 12.2(33)SRB Example

The following is sample output of the **showipv6ospfinterface** command when the **brief** keyword is entered.

```
Router# show ipv6 ospf interface brief

Interface    PID   Area           Intf ID    Cost  State Nbrs F/C
VL0          6     0              21         65535 DOWN  0/0
Se3/0        6     0              14         64    P2P   0/0
Lo1          6     0              20         1     LOOP  0/0
Se2/0        6     6              10         62    P2P   0/0
Tu0          1000  0              19         11111 DOWN  0/0
```

OSPF with Authentication on the Interface Example

The following is sample output from the **showipv6ospfinterface** command with authentication enabled on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Null Authentication Example

The following is sample output from the **showipv6ospfinterface** command with null authentication configured on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Authentication for the Area Example

The following is sample output from the **showipv6ospfinterface** command with authentication configured for the area:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Dynamic Cost Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF cost dynamic is configured.

```
Router1# show ipv6 ospf interface serial 2/0
```

```
Serial2/0 is up, line protocol is up
   Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

OSPF Graceful Restart Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF graceful restart feature is configured:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Graceful Restart p2p timeout in 00:00:19
    Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

Example of an Enabled Protocol

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```
Router# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

show ipv6 ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors in detail (lists all neighbors).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output for the **detail** keyword was updated to display graceful-restart information.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

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

```
Router# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4       1    FULL/  -        00:00:31    14              POS4/0
172.16.3.3       1    FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5       1    FULL/  -        00:00:33    13              ATM3/0
```

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword:

```
Router# show ipv6 ospf neighbor detail
 Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

The table below describes the significant fields shown in the display.

Table 133: show ipv6 ospf neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPF neighbor is known.
Pri; Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software will declare the neighbor dead.

Field	Description
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been re-sent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword, displaying graceful-restart information:

```
Router# show ipv6 ospf neighbor detail
 Neighbor 10.1.1.1
    In the area 0 via interface Ethernet0/0
    Neighbor: interface-id 3, link-local address FE80::A8BB:CCFF:FE00:200
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.1.1.1 BDR is 10.3.3.3
    Options is 0x1C9AD11
    Neighbor graceful restart timer due in 00:01:44
    Last neighbor graceful restart 01:00:19 ago
    Dead timer due in 00:00:36
    Neighbor is up for 00:00:16
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ipv6 ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **s how ipv6 ospf request-list**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the Open Shortest Path First (OSPF) routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf request-list** command is useful in debugging OSPF routing operations.

Examples

The following example shows information about the LSAs requested by the router:

```
Router# show ipv6 ospf request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
 Type    LS ID          ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0        192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0        192.168.255.2   0x800000C8  0      0x000BCA
```

```
 1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
 2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
 2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

The table below describes the significant fields shown in the display.

Table 134: show ipv6 ospf request-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **s how ipv6 ospf retransmission-list**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information only about a specified area.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf retransmission-list** command is useful in debugging Open Shortest Path First (OSPF) routing operations.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
Router# show ipv6 ospf retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

The table below describes the significant fields shown in the display.

Table 135: show ipv6 ospf retransmission-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Link state retransmission due in	Length of time before next link-state transmission.
Queue length	Number of elements in the retransmission queue.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ipv6 ospf statistics

To display Open Shortest Path First for IPv6 (OSPFv6) shortest path first (SPF) calculation statistics, use the **show ipv6 ospf statistics** command in user EXEC or privileged EXEC mode.

show ipv6 ospf statistics [**detail**]

Syntax Description

detail	(Optional) Displays statistics separately for each OSPF area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The **show ipv6 ospf statistics** command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the **show ipv6 ospf statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following example provides detailed statistics for each OSPFv6 area:

```
Router# show ipv6 ospf statistics detail
  Area 0: SPF algorithm executed 3 times
SPF 1 executed 00:06:57 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/0(R)
SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
  Change record R L P
  LSAs changed 4
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

The table below describes the significant fields shown in the display.

Table 136: show ipv6 ospf statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.
Total	Total duration time in milliseconds for the SPF algorithm process.
LSIDs processed	Number of LSAs processed during the SPF calculation: • N--Network LSA. • R--Router LSA. • SA--Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN--Summary Network (SN) LSA. • Stub--Stub links. • X7--External Type-7 (X7) LSA.

show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPF process, use the **s how ipv6 ospf summary-prefix**command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] **summary-prefix**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Examples

The following is sample output from the **show ipv6 ospf summary-prefix** command:

```
Router# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

The table below describes the significant fields shown in the display.

Table 137: show ipv6 ospf summary-prefix Field Descriptions

Field	Description
OSPFv3 Process	Process ID of the router for which information is displayed.
Metric	Metric used to reach the destination router.
Type	Type of link-state advertisement (LSA).
Tag	LSA tag.

show ipv6 ospf timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ipv6 ospf timers rate-limit**command in privileged EXEC mode.

show ipv6 ospf timers rate-limit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **show ipv6 ospf timers rate-limit** command to discover when LSAs in the queue will be sent.

Examples

show ipv6 ospf timers rate-limit Output Example

The following is sample output from the **show ipv6 ospf timers rate-limit**command:

```
Router# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

The table below describes the significant fields shown in the display.

Table 138: show ipv6 ospf timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of the advertising router.
Due in:	When the LSA is scheduled to be sent (in hours:minutes:seconds).

show ipv6 ospf traffic

To display IPv6 Open Shortest Path First Version 3 (OSPFv3) traffic statistics, use the **showipv6ospftraffic**command in privileged EXEC mode.

show ipv6 ospf [*process-id*] **traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) OSPF process ID for which you want traffic statistics (for example, queue statistics, statistics for each interface under the OSPF process, and per OSPF process statistics).
interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.

Command Default

When the **showipv6ospftraffic** command is entered without any arguments, global OSPF traffic statistics are displayed, including queue statistics for each OSPF process, statistics for each interface, and per OSPF process statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPF process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPF process by entering values for the *interface-type* and *interface-number* arguments. To reset counters and clear statistics, use the **clearipv6ospftraffic** command.

Examples

The following example shows the display output for the **showipv6ospftraffic** command for OSPFv3:

```
Router# show ipv6 ospf traffic
OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
```

```
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852
  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface Ethernet0/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960
  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   436
  RX DB des     7                    316
  RX LS req     2                    104
  RX LS upd     9                    692
  RX LS ack     4                    264
  RX Total      33                   1812
  TX Failed     0                    0
  TX Hello      19                   724
  TX DB des     12                   456
  TX LS req     2                    104
  TX LS upd     8                    628
  TX LS ack     6                    296
  TX Total      47                   2208
```

```
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

The network administrator wants to start collecting new statistics, resetting the counters and clearing the traffic statistics by entering the **clearipv6ospftraffic** command as follows:

```
Router# clear ipv6 ospf traffic
```

The table below describes the significant fields shown in the display.

Table 139: show ipv6 ospf traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the **showiptraffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPF hello process for all received OSPF packets.
Router queue	Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.
OSPFv3 header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.
OSPFv3 LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPF link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.

Field	Description
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPF process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPF statistics.

Related Commands

Command	Description
clear ip ospf traffic	Clears OSPFv2 traffic statistics.
clear ipv6 ospf traffic	Clears OSPFv3 traffic statistics.
show ip ospf traffic	Displays OSPFv2 traffic statistics.

show ipv6 ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **s how ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

show ipv6 ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The information displayed by the **show ipv6 ospf virtual-links** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command:

```
Router# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

The table below describes the significant fields shown in the display.

Table 140: show ipv6 ospf virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.

Field	Description
Interface ID	Interface ID and IPv6 address of the router.
Transit area 2	The transit area through which the virtual link is formed.
via interface ATM3/0	The interface through which the virtual link is formed.
Cost of using 1	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:06	When the next hello is expected from the neighbor.

The following sample output from the **show ipv6 ospf virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption.

```
Router# show ipv6 ospf virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
   Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial12/0, Cost of using 64
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/2/4, retransmission queue length 0, number of retransmission 1
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
   Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial11/0, Cost of using 128
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ipv6 pim anycast-RP

To verify IPv6 PIM anycast RP operation, use the **show ipv6 pim anycast-RP** command in user EXEC or privileged EXEC mode.

show ipv6 pim anycast-RP *rp-address*

Syntax Description

rp-address	RP address to be verified.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
Cisco IOS Release 15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
Cisco IOS Release 15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Examples

```
Router# show ipv6 pim anycast-rp 110::1:1:1

Anycast RP Peers For 110::1:1:1   Last Register/Register-Stop received
  20::1:1:1 00:00:00/00:00:00
```

Related Commands

Command	Description
ipv6 pim anycast-RP	Configures the address of the PIM RP for an anycast group range.

show ipv6 pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ipv6 pim bsr** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
election	Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.
rp-cache	Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.
candidate-rp	Displays C-RP state on devices that are configured as C-RPs.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(28)S	The **election**, **rp-cache**, and **candidate-rp** keywords were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **election**, **rp-cache**, and **candidate-rp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.7S	Command output when using the **election** keyword was modified.

Usage Guidelines

Use the **show ipv6 pim bsr** command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP cache is displayed only on the elected BSR device, and information on the C-RP state machine is displayed only on a device configured as a C-RP.

Examples

The following example displays BSM election information:

```
device# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

The table below describes the significant fields shown in the display.

Table 141: show ipv6 pim bsr election Field Descriptions

Field	Description
Scope Range List	Scope to which this BSR information applies.
This system is the Bootstrap Router (BSR)	Indicates this device is the BSR and provides information on the parameters associated with it.
BS Timer	On the elected BSR, the BS timer shows the time in which the next BSM will be originated. On all other devices in the domain, the BS timer shows the time at which the elected BSR expires.
This system is candidate BSR	Indicates this device is the candidate BSR and provides information on the parameters associated with it.

The following example displays information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the FF00::/8 or the default IPv6 multicast range:

```
Device# show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

The following example displays information about the C-RP. This RP has been configured without a specific scope value, so the RP will send C-RP advertisements to all BSRs about which it has learned through BSMs it has received.

```
Device# show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
    Candidate RP: 10::1:1:3
      All Learnt Scoped Zones, Priority 192, Holdtime 150
      Advertisement interval 60 seconds
      Next advertisement in 00:00:33
```

The following example confirms that the IPv6 C-BSR is PIM-enabled. If PIM is disabled on an IPv6 C-BSR interface, or if a C-BSR or C-RP is configured with the address of an interface that does not have PIM enabled, the **show ipv6 pim bsr** command used with the **election** keyword would display that information instead.

```
Device# show ipv6 pim bsr election

PIMv2 BSR information

BSR Election Information
  Scope Range List: ff00::/8
     BSR Address: 2001:DB8:1:1:2
     Uptime: 00:02:42, BSR Priority: 34, Hash mask length: 28
     RPF: FE80::20:1:2,Ethernet1/0
     BS Timer: 00:01:27
```

show ipv6 pim df

To display the designated forwarder (DF)-election state of each interface for each rendezvous point (RP), use the **show ipv6 pim df**command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim df** command to display the state of the DF election for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example displays the DF-election states:

```
Router# show ipv6 pim df
Interface          DF State     Timer          Metrics
Ethernet0/0        Winner       4s 8ms         [120/2]
    RP :200::1
Ethernet1/0        Lose         0s 0ms         [inf/inf]
    RP :200::1
```

The following example shows information on the RP:

```
Router# show ipv6 pim df
Interface          DF State     Timer          Metrics
Ethernet0/0        None:RP LAN 0s 0ms        [inf/inf]
    RP :200::1
Ethernet1/0        Winner       7s 600ms      [0/0]
    RP :200::1
Ethernet2/0        Winner       9s 8ms        [0/0]
    RP :200::1
```

The table below describes the significant fields shown in the display.

Table 142: show ipv6 pim df Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
DF State	The state of the DF election on the interface. The state can be: • Offer • Winner • Backoff • Lose • None:RP LAN The None:RP LAN state indicates that no DF election is taking place on this LAN because the RP is directly connected to this LAN.
Timer	DF election timer.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

show ipv6 pim df winner

To display the designated forwarder (DF)-election winner on each interface for each rendezvous point (RP), use the **show ipv6 pim df winner**command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **df winner** [*interface-type interface-number*] [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp-address	(Optional) RP IPv6 address.

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **show ipv6 pim df winner** command to display the DF election winner for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example shows the DF winner for the IPv6 address 200::1:

```
Router# show ipv6 pim df winner ethernet 1/0 200::1
Interface          Metrics
Ethernet1/0        [120/2]
RP        : 200::1
DF Winner : FE80::A8BB:CCFF:FE00:601
```

The table below describes the significant fields shown in the display.

Table 143: show ipv6 pim df winner Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
Metrics	Routing metrics to the RP announced by the DF.
RP	The IPv6 address of the RP.
DF Winner	The IPv6 address of the DF election winner.

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.

show ipv6 pim group-map

To display an IPv6 Protocol Independent Multicast (PIM) group mapping table, use the **show ipv6 pim group-map** command in user EXEC or privileged EXEC mode.

{**show ipv6 pim** [**vrf** *vrf-name*] **group-map** [{*group-namegroup-address*}] | [{*group-rangegroup-mask*}] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-name | *group-address*	(Optional) IPv6 address or name of the multicast group.
group-range | *group-mask*	(Optional) Group range list. Includes group ranges with the same prefix or mask length.
info-source	(Optional) Displays all mappings learned from a specific source, such as the bootstrap router (BSR) or static configuration.
bsr	Displays ranges learned through the BSR.
default	Displays ranges enabled by default.
embedded-rp	Displays group ranges learned through the embedded rendezvous point (RP).
static	Displays ranges enabled by static configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.0(28)S	The *group-range* and *group-mask*arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.2(25)S	The *group-range* and *group-mask*arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.3(11)T	The *group-range* and *group-mask*arguments were added, and the **info-source bsr**, **static**, and **default** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 pim group-map** command to find all group mappings installed by a given source of information, such as BSR or static configuration.

You can also use this command to find which group mapping a router at a specified IPv6 group address is using by specifying a group address, or to find an exact group mapping entry by specifying a group range and mask length.

Examples

The following is sample output from the **show ipv6 pim group-map**command:

```
Router# show ipv6 pim group-map
FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
      Info source:Static
      Uptime:00:09:42, Groups:0
```

The table below describes the significant fields shown in the display.

Table 144: show ipv6 pim group-map Field Descriptions

Field	Description
RP	Address of the RP router if the protocol is sparse mode or bidir.
Protocol	Protocol used: sparse mode (SM), Source Specific Multicast (SSM), link-local (LL), or NOROUTE (NO). LL is used for the link-local scoped IPv6 address range (ff[0-f]2::/16). LL is treated as a separate protocol type, because packets received with these destination addresses are not forwarded, but the router might need to receive and process them. NOROUTE or NO is used for the reserved and node-local scoped IPv6 address range (ff[0-f][0-1]::/16). These addresses are nonroutable, and the router does not need to process them.
Groups	How many groups are present in the topology table from this range.
Info source	Mappings learned from a specific source; in this case, static configuration.
Uptime	The uptime for the group mapping displayed.

The following example displays the group mappings learned from BSRs that exist in the PIM group-to-RP or mode-mapping cache. The example shows the address of the BSR from which the group mappings have been learned and the associated timeout.

```
Router# show ipv6 pim group-map info-source bsr
FF00::/8*
    SM, RP: 20::1:1:1
    RPF: Et1/0,FE80::A8BB:CCFF:FE03:C202
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
FF00::/8*
    SM, RP: 10::1:1:3
    RPF: Et0/0,FE80::A8BB:CCFF:FE03:C102
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
```

show ipv6 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
state-on	(Optional) Displays interfaces with PIM enabled.
state-off	(Optional) Displays interfaces with PIM disabled.
type number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	The **state-on** and **state-off**keywords were added.
12.3(4)T	The **state-on** and **state-off**keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	Command output was modified to display passive interface information.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **show ipv6 pim interface** command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

Examples

The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword:

```
Router# show ipv6 pim interface state-on
Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior
```

```
Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

The table below describes the significant fields shown in the display.

Table 145: show ipv6 pim interface Field Descriptions

Field	Description
Interface	Interface type and number that is configured to run PIM.
PIM	Whether PIM is enabled on an interface.
Nbr Count	Number of PIM neighbors that have been discovered through this interface.
Hello Intvl	Frequency, in seconds, of PIM hello messages.
DR	IP address of the designated router (DR) on a network.
Address	Interface IP address of the next-hop router.

The following is sample output from the **show ipv6 pim interface** command, modified to display passive interface information:

```
Router(config)# show ipv6 pim interface gigabitethernet0/0/0

    Interface              PIM   Nbr   Hello  DR  BFD
                           Count Intvl Prior

    GigabitEthernet0/0/0   on/P  0     30     1   On
       Address: FE80::A8BB:CCFF:FE00:9100
       DR     : this system
```

The table below describes the significant change shown in the display.

Table 146: show ipv6 pim interface Field Description

Field	Description
PIM	Whether PIM is enabled on an interface. When PIM passive mode is used, a "P" is displayed in the output.

Related Commands

Command	Description
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

show ipv6 pim join-prune statistic

To display the average join-prune aggregation for the most recently aggregated 1000, 10,000, and 50,000 packets for each interface, use the **show ipv6 pim join-prune statistic** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

When Protocol Independent Multicast (PIM) sends multiple joins and prunes simultaneously, it aggregates them into a single packet. The **show ipv6 pim join-prune statistic** command displays the average number of joins and prunes that were aggregated into a single packet over the last 1000 PIM join-prune packets, over the last 10,000 PIM join-prune packets, and over the last 50,000 PIM join-prune packets.

Examples

The following example provides the join/prune aggregation on Ethernet interface 0/0/0:

```
Router# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface             Transmitted             Received
Ethernet0/0/0      0    / 0    / 0          1    / 0    / 0
```

The table below describes the significant fields shown in the display.

Table 147: show ipv6 pim join-prune statistics Field Descriptions

Field	Description
Interface	The interface from which the specified packets were transmitted or on which they were received.
Transmitted	The number of packets transmitted on the interface.
Received	The number of packets received on the interface.

show ipv6 pim limit

To display Protocol Independent Multicast (PIM) interface limit, use the **show ipv6 pim limit** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface	(Optional) Specific interface for which limit information is provided.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **show ipv6 pim limit** command checks interface statistics for limits. If the optional *interface* argument is enabled, only information for the specified interface is shown.

Examples

The following example displays s PIM interface limit information:

```
Router# show ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

show ipv6 pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco software, use the **show ipv6 pim neighbor** command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
detail	(Optional) Displays the additional addresses of the neighbors learned, if any, through the routable address hello option.
interface-type interface-number	(Optional) Interface type and number.
count	(Optional) Displays neighbor counts on each interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf***vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 pim neighbor** command displays which routers on the LAN are configured for PIM.

Examples

The following is sample output from the **show ipv6 pim neighbor** command using the detail keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
Router# show ipv6 pim neighbor detail

Neighbor Address(es)       Interface          Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:401   Ethernet0/0        01:34:16  00:01:16 1      B
60::1:1:3
```

```
FE80::A8BB:CCFF:FE00:501   Ethernet0/0        01:34:15  00:01:18 1      B
60::1:1:4
```

The table below describes the significant fields shown in the display.

Table 148: show ipv6 pim neighbor Field Descriptions

Field	Description
Neighbor addresses	IPv6 address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table.
Expires	How long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.
DR	Indicates that this neighbor is a designated router (DR) on the LAN.
pri	DR priority used by this neighbor.
Bidir	The neighbor is capable of PIM in bidirectional mode.

Related Commands

Command	Description
show ipv6 pim interfaces	Displays information about interfaces configured for PIM.

show ipv6 pim range-list

To display information about IPv6 multicast range lists, use the **show ipv6 pim range-list**command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **range-list** [**config**] [{*rp-addressrp-name*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
config	(Optional) The client. Displays the range lists configured on the router.
rp-address | *rp-name*	(Optional) The address of a Protocol Independent Multicast (PIM) rendezvous point (RP).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 pim range-list** command displays IPv6 multicast range lists on a per-client and per-mode basis. A client is the entity from which the specified range list was learned. The clients can be config, and the modes can be Source Specific Multicast (SSM) or sparse mode (SM).

Examples

The following is sample output from the **show ipv6 pim range-list**command:

```
Router# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
```

```
 FF37::/32 Up:00:26:33
 FF38::/32 Up:00:26:33
 FF39::/32 Up:00:26:33
 FF3A::/32 Up:00:26:33
 FF3B::/32 Up:00:26:33
 FF3C::/32 Up:00:26:33
 FF3D::/32 Up:00:26:33
 FF3E::/32 Up:00:26:33
 FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

The table below describes the significant fields shown in the display.

Table 149: show ipv6 pim range-list Field Descriptions

Field	Description
config	Config is the client.
SSM	Protocol being used.
FF33::/32	Group range.
Up:	Uptime.

show ipv6 pim topology

To display Protocol Independent Multicast (PIM) topology table information for a specific group or all groups, use the **show ipv6 pim topology** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **topology** [{*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
groupname-or-address	(Optional) IPv6 address or name of the multicast group.
sourcename-or-address	(Optional) IPv6 address or name of the source.
link-local	(Optional) Displays the link-local groups.
route-count	(Optional) Displays the number of routes in PIM topology table.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was modified. The **link-local** keyword was added.
12.3(4)T	This command was modified. The **link-local** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

This command shows the PIM topology table for a given group--(*, G), (S, G), and (S, G) Rendezvous Point Tree (RPT)-- as internally stored in a PIM topology table. The PIM topology table may have various entries for a given group, each with its own interface list. The resulting forwarding state is maintained in the Multicast

Routing Information Base (MRIB) table, which shows which interface the data packet should be accepted on and which interfaces the data packet should be forwarded to for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

The **route-count**keyword shows the count of all entries, including link-local entries.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols (such as PIM), local membership protocols (such as Multicast Listener Discovery [MLD]), and the multicast forwarding engine of the system.

For example, an interface is added to the (*, G) entry in PIM topology table upon receipt of an MLD report or PIM (*, G) join message. Similarly, an interface is added to the (S, G) entry upon receipt of the MLD INCLUDE report for the S and G or PIM (S, G) join message. Then PIM installs an (S, G) entry in the MRIB with the immediate olist (from (S, G)) and the inherited olist (from (*, G)). Therefore, the proper forwarding state for a given entry (S, G) can be seen only in the MRIB or the MFIB, not in the PIM topology table.

Examples

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

```
Router# show ipv6 pim topology
IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH
(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

The table below describes the significant fields shown in the display.

Table 150: show ipv6 pim topology Field Descriptions

Field	Description
Entry flags: KAT	The keepalive timer (KAT) associated with a source is used to keep track of two intervals while the source is alive. When a source first becomes active, the first-hop router sets the keepalive timer to 3 minutes and 30 seconds, during which time it does not probe to see if the source is alive. Once this timer expires, the router enters the probe interval and resets the timer to 65 seconds, during which time the router assumes the source is alive and starts probing to determine if it actually is. If the router determines that the source is alive, the router exits the probe interval and resets the keepalive timer to 3 minutes and 30 seconds. If the source is not alive, the entry is deleted at the end of the probe interval.
AA, PA	The assume alive (AA) and probe alive (PA) flags are set when the router is in the probe interval for a particular source.

Field	Description
RR	The register received (RR) flag is set on the (S, G) entries on the Route Processor (RP) as long as the RP receives registers from the source Designated Router (DR), which keeps the source state alive on the RP.
SR	The sending registers (SR) flag is set on the (S, G) entries on the DR as long as it sends registers to the RP.

Related Commands

Command	Description
show ipv6 mrib client	Displays information about the clients of the MRIB.
show ipv6 mrib route	Displays MRIB route information.

show ipv6 pim traffic

To display the Protocol Independent Multicast (PIM) traffic counters, use the **show ipv6 pim traffic** command in user EXEC or privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **traffic**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **show ipv6 pim traffic** command to check if the expected number of PIM protocol messages have been received and sent.

Examples

The following example shows the number of PIM protocol messages received and sent.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29
                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0
Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
```

```
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

The table below describes the significant fields shown in the display.

Table 151: show ipv6 pim traffic Field Descriptions

Field	Description
Elapsed time since counters cleared	Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.
Valid PIM Packets	Number of valid PIM packets received and sent.
Hello	Number of valid hello messages received and sent.
Join-Prune	Number of join and prune announcements received and sent.
Register	Number of PIM register messages received and sent.
Register Stop	Number of PIM register stop messages received and sent.
Assert	Number of asserts received and sent.

show ipv6 pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and de-encapsulation tunnels on an interface, use the **show ipv6 pim tunnel**command in privileged EXEC mode.

show ipv6 pim [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
interface-type interface-number	(Optional) Tunnel interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

If you use the **show ipv6 pim tunnel** command without the optional *interface* keyword, information about the PIM register encapsulation and de-encapsulation tunnel interfaces is displayed.

The PIM encapsulation tunnel is the register tunnel. An encapsulation tunnel is created for every known rendezvous point (RP) on each router. The PIM decapsulation tunnel is the register decapsulation tunnel. A decapsulation tunnel is created on the RP for the address that is configured to be the RP address.

Examples

The following is sample output from the **show ipv6 pim tunnel**command on the RP:

```
Router# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:100::1
Tunnel0*
```

```
 Type  :PIM Decap
 RP    :100::1
 Source: -
```

The following is sample output from the **show ipv6 pim tunnel**command on a non-RP:

```
Router# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:2001::1:1:1
```

The table below describes the significant fields shown in the display.

Table 152: show ipv6 pim tunnel Field Descriptions

Field	Description
Tunnel0*	Name of the tunnel.
Type	Type of tunnel. Can be PIM encapsulation or PIM de-encapsulation.
source	Source address of the router that is sending encapsulating registers to the RP.

show ipv6 policy

To display the IPv6 policy-based routing (PBR) configuration, use the **show ipv6 policy** command in user EXEC or privileged EXEC mode.

show ipv6 policy

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

IPv6 policy matches will be counted on route maps, as is done in IPv4. Therefore, IPv6 policy matches can also be displayed on the **show route-map** command.

Examples

The following example displays the PBR configuration:

```
Device# show ipv6 policy

Interface                  Routemap
Ethernet0/0                src-1
```

The table below describes the significant fields shown in the display.

Field	Description
Interface	Interface type and number that is configured to run Protocol-Independent Multicast (PIM).
Routemap	The name of the route map on which IPv6 policy matches were counted.

Related Commands

Command	Description
show route-map	Displays all route maps configured or only the one specified.

show ipv6 port-map

To verify port-to-application mapping (PAM) configuration, use the **show ipv6 port-map**command in user EXEC or privileged EXEC mode.

show ipv6 port-map [{*application* | **port** *port-number*}]

Syntax Description

application	(Optional) Specifies the name of the application used in port mapping.
port *port-number*	(Optional) Specifies the port number that maps to the application.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 port-map** command displays the entire IPv6 port-mapping table or specific port-mapping information of a particular port number or application (protocol). Enabling the **show ipv6 port-map** command displays the entire IPv6 PAM table, including system-defined, user-defined, and host-specific port-mapping configurations.

To display port-mapping details of a specific port number, use the **show ipv6 port-map** command with the **port***port-number* keyword and argument.

To display the port-mapping details of a specific application, use the **show ipv6 port-map** command with the *application* argument.

Examples

The following example displays the FTP application's PAM information:

```
Router# show ipv6 port-map ftp
```

The following example displays PAM information at port number 21:

```
Router# show ipv6 port-map port 21
```

Related Commands

Command	Description
ipv6 port-map	Establishes PAM for the system.

show ipv6 prefix-list

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list**command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [{**detail** | **summary**}] [*list-name*]
show ipv6 prefix-list *list-name* *ipv6-prefix/prefix-length* [{**longer** | **first-match**}]
show ipv6 prefix-list *list-name* **seq** *seq-num*

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.
list-name	(Optional) The name of a specific IPv6 prefix list.
ipv6-prefix	All prefix list entries for the specified IPv6 network. 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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer	(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given *ipv6-prefix* / *prefix-length*values.
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given *ipv6-prefix* / *prefix-length*values.
seq *seq-num*	The sequence number of the IPv6 prefix list entry.

Command Default

Displays information about all IPv6 prefix lists.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show ipv6 prefix-list** command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

Examples

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

The table below describes the significant fields shown in the display.

Table 153: show ipv6 prefix-list Field Descriptions

Field	Description
Prefix list with the latest deletion/insertion:	Prefix list that was last modified.
count	Number of entries in the list.
range entries	Number of entries with matching range.
sequences	Sequence number for the prefix entry.
refcount	Number of objects currently using this prefix list.
seq	Entry number in the list.
permit, deny	Granting status.
hit count	Number of matches for the prefix entry.

The following example shows the output of the **show ipv6 prefix-list** command with the **summary**keyword:

```
Router# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
```

```
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list description	Adds a text description of an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
remark (prefix-list)	Adds a comment for an entry in a prefix list.

show ipv6 protocols

To display the parameters and the current state of the active IPv6 routing protocol processes, use the **show ipv6 protocols** command in user EXEC or privileged EXEC mode.

show ipv6 protocols [**summary**]

Syntax Description

summary	(Optional) Displays the configured routing protocol process names.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified. The command output was enhanced to provide Enhanced Interior Gateway Routing Protocol (EIGRP) information, including the vector metric.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.6	This command was modified. The command output was enhanced to include information about EIGRP IPv6 Nonstop Forwarding (NSF).
15.2(2)S	This command was modified. The command output was enhanced to include information about EIGRP IPv6 NSF.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The information displayed by the **show ipv6 protocols** command is useful in debugging routing operations.

Examples

The following sample output from the **show ipv6 protocols** command displays Intermediate System-to-Intermediate System (IS-IS) routing protocol information:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16  advertised with metric 0
    L2: 44::/16  advertised with metric 20
    L2: 66::/16  advertised with metric 10
    L2: 77::/16  advertised with metric 10
```

The table below describes the significant fields shown in the display.

Table 154: show ipv6 protocols Field Descriptions for IS-IS Processes

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Interfaces	Specifies the interfaces on which the IPv6 IS-IS protocol is configured.
Redistribution	Lists the protocol that is being redistributed.
Inter-area redistribution	Lists the IS-IS levels that are being redistributed into other levels.
using prefix-list	Names the prefix list used in the interarea redistribution.
Address Summarization	Lists all the summary prefixes. If the summary prefix is being advertised, "advertised with metric *x*" will be displayed after the prefix.

The following sample output from the **show ipv6 protocols** command displays the Border Gateway Protocol (BGP) information for autonomous system 30:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
```

```
    Address                    FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1            5       7    200
    2001:DB8:0:ABCD::2                               rmap-in    rmap-out
    2001:DB8:0:ABCD::3                               rmap-in    rmap-out
```

The table below describes the significant fields shown in the display.

Table 155: show ipv6 protocols Field Descriptions for BGP Process

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Redistribution	Lists the protocol that is being redistributed.
Address	Neighbor IPv6 address.
FiltIn	AS-path filter list applied to input.
FiltOut	AS-path filter list applied to output.
Weight	Neighbor weight value used in BGP best path selection.
RoutemapIn	Neighbor route map applied to input.
RoutemapOut	Neighbor route map applied to output.

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

```
Device# show ipv6 protocols summary

Index Process Name
0     connected
1     static
2     rip myrip
3     bgp 30
```

The following sample output from the **show ipv6 protocols** command displays the EIGRP information including the vector metric and EIGRP IPv6 NSF:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
     NSF signal timer is 15s
     NSF converge timer is 65s
  Router-ID: 10.1.2.2
  Topology : 0 (base)
```

```
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 0
    Total Redist Count: 0

  Interfaces:
  Redistribution:
    None
```

The following example displays IPv6 protocol information after configuring redistribution in an Open Shortest Path First (OSPF) domain:

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
  Interfaces:
    Ethernet0/1
    Loopback9
  Redistribution:
    Redistributing protocol ospf 1 (internal)
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Ethernet0/0
  Redistribution:
    None
```

IPv6 Commands: show ipv6 ri to si

show ipv6 rip

To display information about current IPv6 Routing Information Protocol (RIP) processes, use the **show ipv6 rip** command in user EXEC or privileged EXEC mode.

Cisco IOS XE Release 3.9S, Cisco IOS Release 15.3(2)S, and Later Releases

show ipv6 rip [*name*] [**vrf** *vrf-name*] [{**database** | **next-hops**}]

Releases Prior to Cisco IOS XE Release 3.9S and Cisco IOS Release 15.3(2)S

show ipv6 rip [*name*] [{**database** | **next-hops**}]

Syntax Description

name	(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes are displayed.
vrf *vrf-name*	(Optional) Displays information about the specified Virtual Routing and Forwarding (VRF) instance.
database	(Optional) Displays information about entries in the specified RIP IPv6 routing table.
next-hops	(Optional) Displays information about the next hop addresses for the specified RIP IPv6 process. If no RIP process name is specified, the next-hop addresses for all RIP IPv6 processes are displayed.

Command Default

Information about all current IPv6 RIP processes is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The *name* argument and the **database** and **next-hops** keywords were added.
12.2(13)T	The command was modified. The *name* argument, and the **database** and **next-hops** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was implemented on Cisco 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was modified. The **vrf** *vrf-name* keyword/argument pair was added.
15.3(2)S	This command was integrated into Cisco IOS Release 15.3(2)S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Examples

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

```
Device# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
     Administrative distance is 25. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
  Redistribution:
RIP process "two", port 521, multicast-group FF02::9, pid 61
     Administrative distance is 120. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 0
  Interfaces:
    None
  Redistribution:
```

The table below describes the significant fields shown in the display.

Table 156: show ipv6 rip Field Descriptions

Field	Description
RIP process	The name of the RIP process.
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
pid	The process identification number (pid) assigned to the RIP process.
Administrative distance	Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value.
Updates	The value (in seconds) of the update timer.

Field	Description
expire	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

The following is sample output from the **show ipv6 rip database** command.

```
Device# show ipv6 rip one database

RIP process "one", local RIB
 2001:72D:1000::/64, metric 2
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
 2001:72D:2000::/64, metric 2, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
 2001:72D:3000::/64, metric 2, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
     Ethernet1/2001:DB8::1, expires in 120 secs
 2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
     Ethernet2/2001:DB8:0:ABCD::1
 3004::/64, metric 2 tag 2A, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
```

The table below describes the significant fields shown in the display.

Table 157: show ipv6 rip database Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:72D:1000::/64	The IPv6 route prefix.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet2/2001:DB8:0:ABCD::1	Interface and LL next hop through which the IPv6 route was learned.
expires in	The interval (in seconds) before the route expires.
advertise	For an expired route, the value (in seconds) during which the route will be advertised as expired.

Field	Description
hold	The value (in seconds) of the hold-down timer.
tag	Route tag.

The following is sample output from the **show ipv6 rip next-hops** command.

```
Device# show ipv6 rip one next-hops

RIP process "one", Next Hops
  FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
  FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]
```

The table below describes the significant fields shown in the display.

Table 158: show ipv6 rip next-hops Field Descriptions

Field	Description
RIP process	The name of the RIP process.
2001:DB8:0:1::1/Ethernet4/2	The next-hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes or explicit next hops received in IPv6 RIP advertisements. **Note** An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.
[1 routes]	The number of routes in the IPv6 RIP routing table using the specified next hop.

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

```
Device# show ipv6 rip vrf red

     RIP VRF "red", port 521, multicast-group 2001:DB8::/32, pid 295
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 99, trigger updates 3
     Full Advertisement 0, Delayed Events 0
  Interfaces:
    Ethernet0/1
    Loopback2
  Redistribution:
    None
```

The table below describes the significant fields shown in the display.

Table 159: show ipv6 rip vrf Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.

Field	Description
port	The port that the RIP process is using.
multicast-group	The IPv6 multicast group of which the RIP process is a member.
Administrative distance	Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value.
Updates	The value (in seconds) of the update timer.
expires after	The interval (in seconds) in which updates expire.
Holddown	The value (in seconds) of the hold-down timer.
garbage collect	The value (in seconds) of the garbage-collect timer.
Split horizon	The split horizon state is either on or off.
poison reverse	The poison reverse state is either on or off.
Default routes	The origination of a default route into RIP. Default routes are either generated or not generated.
Periodic updates	The number of RIP update packets sent on an update timer.
trigger updates	The number of RIP update packets sent as triggered updates.

The following is sample output from **show ipv6 rip vrf next-hops** command:

```
Device# show ipv6 rip vrf blue next-hops

     RIP VRF "blue", local RIB
      AAAA::/64, metric 2, installed
     Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00, expires in 177 secs
```

Table 160: show ipv6 rip vrf next-hops Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
metric	Metric for the route.
installed	Route is installed in the IPv6 routing table.
Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00	The next hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes, or explicit next hops received in IPv6 RIP advertisements. **Note** An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.

Field	Description
expires in	The interval (in seconds) before the route expires.

The following is sample output from **show ipv6 rip vrf database** command:

```
Device# show ipv6 rip vrf blue database

        RIP VRF "blue", Next Hops
       FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

Table 161: show ipv6 rip vrf database Field Descriptions

Field	Description
RIP VRF	The name of the RIP VRF.
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0	Interface and LL next hop through which the IPv6 route was learned.
1 paths	Indicates the number of unique paths to this router that exist in the routing table.

Related Commands

Command	Description
clear ipv6 rip	Deletes routes from the IPv6 RIP routing table.
debug ipv6 rip	Displays the current contents of the IPv6 RIP routing table.
ipv6 rip vrf-mode enable	Enables VRF-aware support for IPv6 RIP.

show ipv6 route

To display contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

show ipv6 route [{*ipv6-address* | *ipv6-prefix*/*prefix-length* [{**longer-prefixes**}] | [{*protocol*}] | [**repair**] | [{**updated** [{**boot-up**}] [{*day month*}] [{*time*}]}] | **interface** *type number* | **nd** | **nsf** | **table** *table-id* | **watch**}]

Syntax Description

ipv6-address	(Optional) Displays routing information for a specific IPv6 address.
ipv6-prefix	(Optional) Displays routing information for a specific IPv6 network.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **local**, **mobile**, or **static**. If you specify a routing protocol, use one of the following keywords: **bgp**, **isis**, **eigrp**, **ospf**, or **rip**.
repair	(Optional) Displays routes with repair paths.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since bootup.
day month	(Optional) Displays routes since the specified day and month.
time	(Optional) Displays routes since the specified time, in *hh:mm* format.
interface	(Optional) Displays information about the interface.
type	(Optional) Interface type.
number	(Optional) Interface number.
nd	(Optional) Displays only routes from the IPv6 Routing Information Base (RIB) that are owned by Neighbor Discovery (ND).
nsf	(Optional) Displays routes in the nonstop forwarding (NSF) state.
repair	(Optional)
table *table-id*	(Optional) Displays IPv6 RIB table information for the specified table ID. The table ID must be in hexadecimal format. The range is from 0 to 0-0xFFFFFFFF.
watch	(Optional) Displays information about route watchers.

Command Default If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. The **isis** keyword was added, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were included in the command output.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The timer information was removed, and an indicator was added to display IPv6 Multiprotocol Label Switching (MPLS) interfaces.
12.2(13)T	This command was modified. The timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(14)S	This command was modified. The **longer-prefixes** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **table**, **nsf**, **watch**, and **updated** keywords and the *day, month, table-id*, and *time* arguments were added.
15.2(2)S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
15.1(1)SY	The **nd** keyword was added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only the specified type of route is displayed. When the **interface** keyword and *type* and *number* arguments are specified, only routes for the specified interface are displayed.

Examples

The following is sample output from the **show ipv6 route** command when no keywords or arguments are specified:

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
     via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
     via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
     via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
     via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
     via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

The table below describes the significant fields shown in the display.

Table 162: show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • B—BGP derived • C—Connected • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived • L—Local • R—RIP derived • S—Static

Field	Description
2001:DB8:4::2/48	Indicates the IPv6 prefix of the remote network.
[20/0]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via FE80::A8BB:CCFF:FE02:8B00	Specifies the address of the next device to the remote network.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route bgp** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B   2001:DB8:4::4/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the **show ipv6 route local** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
     via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

The following is sample output from the **show ipv6 route** command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

```
Device# show ipv6 route
```

```
IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   2001:DB8::/64 [200/0]
     via ::FFFF:172.16.0.1
     via ::FFFF:172.30.30.1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 route shortcut

To display the IPv6 routes that contain shortcuts, use the **show ipv6 route shortcut**command in privileged EXEC mode.

show ipv6 route shortcut

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 information about shortcuts for all active routing tables is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

The **show ipv6 route shortcut** command displays only the routes that have overriding shortcut paths.

Examples

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

```
Router# show ipv6 route shortcut
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - Neighbor Discovery, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S 7000:1::/64 [1/0]
    via 4000:1:1::1, Ethernet1/1 [Shortcut]
    via 5000:1:1::1, Ethernet1/1 [Shortcut]
    via Ethernet1/1, directly connected
S 8000:1:1::/64 [1/0]
    via 6000:1:1::1, Ethernet0/1 [Shortcut]
    via Ethernet0/0, directly connected
```

The table below describes the significant fields shown in the display.

Table 163: show ipv6 route shortcut Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • C--Connected • L--Local • S--Static • R--RIP derived • B--BGP derived • I1--ISIS L1--Integrated IS-IS Level 1 derived • I2--ISIS L2--Integrated IS-IS Level 2 derived • IA--ISIS interarea--Integrated IS-IS interarea derived
S 7000:1::/64 [1/0]	Indicates paths that may be shortcut paths.
via 4000:1:1::1, Ethernet1/1	Indicates a path that may be a shortcut path.
via 5000:1:1::1, Ethernet1/1 [Shortcut]	Indicates a path that may be a shortcut path.
via Ethernet1/1, directly connected	Shows routes connected to the router directly.

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 route summary

To display the current contents of the IPv6 routing table in summary format, use the **show ipv6 route summary**command in user EXEC or privileged EXEC mode.

show ipv6 route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

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

```
Router# show ipv6 route summary
IPv6 Routing Table Summary - 257 entries
  37 local, 35 connected, 25 static, 0 RIP, 160 BGP
  Number of prefixes:
    /16: 1, /24: 46, /28: 10, /32: 5, /35: 25, /40: 1, /48: 63, /64: 19
    /96: 15, /112: 1, /126: 31, /127: 4, /128: 36
```

The table below describes the significant fields shown in the display.

Table 164: show ipv6 route summary Field Descriptions

Field	Description
entries	Number of entries in the IPv6 routing table.

Field	Description
Route source	Number of routes that are present in the routing table for each route source, which can be local routes, connected routes, static routes, a routing protocol, prefix and address or name, and longer prefixes and address or name. Routing protocols can include RIP, IS-IS, OSPF, and BGP. Other route sources can be connected, local, static, or a specific interface.
Number of prefixes:	Number of routing table entries for given prefix length.

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.

show ipv6 route vrf

To display IPv6 routing table information associated with a VPN routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in user EXEC or privileged EXEC mode.

show ipv6 route vrf {*vrf-namevrf-number*}[**tag** {*tag-value* | *tag-value-dotted-decimal* [{*mask*}]}]

Syntax Description

vrf-name	Name assigned to the VRF.
vrf-number	Hexadecimal number assigned to the VRF.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Displays route tag value in plain decimals.
tag-value-dotted-decimal	(Optional) Displays route tag values in dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.2(2)S	This command was integrated into Cisco IOS Release 15.2(2)S. The **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S. The **tag** keyword and the *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain decimals or dotted decimals in the command output.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following sample output from the **show ipv6 route vrf** command displays information about the IPv6 routing table associated with VRF1:

```
Device# show ipv6 route vrf VRF1
```

```
IPv6 Routing Table VRF1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:DB8:4::2/48 [0/0]
     via ::, FastEthernet0/0
L   2001:DB8:4::3/48 [0/0]
     via ::, FastEthernet0/0
B   2001:DB8:4::4/48 [200/0]
     via ::FFFF:192.168.1.4,
B   2001:DB8:4::5/48 [20/1]
     via 2001:8::1,
C   2001:DB8:4::6/48 [0/0]
     via ::, Loopback1
L   2001:DB8:4::7/48 [0/0]
     via ::, Loopback1
```

The following sample output from the **show ip route vrf** *vrf-name* **tag** command displays information about tagged IPv6 routes in vrf1:

```
Device# show ipv6 route vrf vrf1 tag 0.0.0.6

IPv6 Routing Table - vrf1 - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
Routing entry for 2001::/32
  Known via "static", distance 1, metric 0
  Tag 0.0.0.6
  Route count is 1/1, share count 0
  Routing paths:
    directly connected via Null0
      Last updated 00:00:23 ago
```

The table below describes the significant fields shown in the displays.

Table 165: show ipv6 route vrf Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • I—IS-IS derived • L—Local • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route
via ::, FastEthernet0/0	Indicates how the route was derived.
Tag	Identifies the tag associated with the remote network.

show ipv6 routers

To display IPv6 router advertisement (RA) information received from on-link devices, use the **show ipv6 routers** command in user EXEC or privileged EXEC mode.

show ipv6 routers [*interface-type interface-number*] [**conflicts**] [**vrf vrf-name**] [**detail**]

Syntax Description

interface -type	(Optional) Specifies the Interface type.
interface -number	(Optional) Specifies the Interface number.
conflicts	(Optional) Displays RAs that differ from the RAs configured for a specified interface.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
detail	(Optional) Provides detail about the eligibility of the neighbor for election as the default device.

Command Default

When an interface is not specified, on-link RA information is displayed for all interface types. (The term *onl-ink* refers to a locally reachable address on the link.)

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by other devices.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(2)SE	The **vrf** *vrf-name* keyword and argument pair and the **detail** keyword were added.

Usage Guidelines

Devices that advertise parameters that differ from the RA parameters configured for the interface on which the RAs are received are marked as conflicting.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an IPv6 interface type and number:

```
Device# show ipv6 routers

Device FE80::83B3:60A4 on Tunnel5, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Device FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

The following sample output shows a single neighboring device that is advertising a high default device preference and is indicating that it is functioning as a Mobile IPv6 home agent on this link.

```
Device# show ipv6 routers

IPV6 ND Routers (table: default)
  Device FE80::100 on Ethernet0/0, last update 0 min
  Hops 64, Lifetime 50 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=1, Preference=High
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::100/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

The following table describes the significant fields shown in the displays.

Table 166: show ipv6 routers Field Descriptions

Field	Description
Hops	The configured hop limit value for the RA.
Lifetime	The configured lifetime value for the RA. A value of 0 indicates that the device is not a default device. A value other than 0 indicates that the device is a default device.
AddrFlag	If the value is 0, the RA received from the device indicates that addresses are not configured using the stateful autoconfiguration mechanism. If the value is 1, the addresses are configured using this mechanism.
OtherFlag	If the value is 0, the RA received from the device indicates that information other than addresses is not obtained using the stateful autoconfiguration mechanism. If the value is 1, other information is obtained using this mechanism. (The value of OtherFlag can be 1 only if the value of AddrFlag is 1.)
MTU	The maximum transmission unit (MTU).
HomeAgentFlag=1	The value can be either 0 or 1. A value of 1 indicates that the device from which the RA was received is functioning as a mobile IPv6 home agent on this link, and a value of 0 indicates it is not functioning as a mobile IPv6 home agent on this link.
Preference=High	The DRP value, which can be high, medium, or low.

Field	Description
Retransmit time	The configured RetransTimer value. The time value to be used on this link for neighbor solicitation transmissions, which are used in address resolution and neighbor unreachability detection. A value of 0 means the time value is not specified by the advertising device.
Prefix	A prefix advertised by the device. Also indicates if on-link or autoconfig bits were set in the RA message.
Valid lifetime	The length of time (in seconds) relative to the time the advertisement is sent that the prefix is valid for the purpose of on-link determination. A value of -1 (all ones, 0xffffffff) represents infinity.
preferred lifetime	The length of time (in seconds) relative to the time the advertisements is sent that addresses generated from the prefix via address autoconfiguration remain valid. A value of -1 (all ones, 0xffffffff) represents infinity.

When the *interface-type* and *interface-number* arguments are specified, RA details about that specific interface are displayed. The following is sample output from the **show ipv6 routers** command when entered with an interface type and number:

```
Device# show ipv6 routers tunnel 5

Device FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
```

Entering the **conflicts** keyword with the **show ipv6 routers** command displays information for devices that are advertising parameters different from the parameters configured for the interface on which the advertisements are being received, as the following sample output shows:

```
Device# show ipv6 routers conflicts

Device FE80::203:FDFF:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2003::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
Device FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2001::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
```

Use of the **detail** keyword provides information about the preference rank of the device, its eligibility for election as default device, and whether the device has been elected:

```
Device# show ipv6 routers detail

Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
  Rank 0x811 (elegible), Default Router
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=0, Preference=Medium, trustlevel = 0
  Reachable time 0 (unspecified), Retransmit time 0 (unspecified)
```

```
Prefix 2001::/64 onlink autoconfig
  Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 rpf

To check Reverse Path Forwarding (RPF) information for a given unicast host address and prefix, use the **show ipv6 rpf** command in user EXEC or privileged EXEC mode.

show ipv6 rpf {*source-vrf* [*access-list*] | **vrf** *receiver-vrf*{*source-vrf* [*access-list*] | **select**}}

Syntax Description

source-vrf	Name or address of the virtual routing and forwarding (VRF) on which lookups are to be performed.
receiver-vrf	Name or address of the VRF in which the lookups originate.
access-list	Name or address of access control list (ACL) to be applied to the group-based VRF selection policy.
vrf	Displays information about the VRF instance.
select	Displays group-to-VRF mapping information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(4)M	The **vrf** *receiver-vrf* keyword and argument were added.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **show ipv6 rpf**command displays information about how IPv6 multicast routing performs Reverse Path Forwarding (RPF). Because the router can find RPF information from multiple routing tables (for example, unicast Routing Information Base [RIB], multiprotocol Border Gateway Protocol [BGP] routing table, or static mroutes), the **show ipv6 rpf**command to display the source from which the information is retrieved.

Examples

The following example displays RPF information for the unicast host with the IPv6 address of 2001::1:1:2:

```
Router# show ipv6 rpf 2001::1:1:2
RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

The table below describes the significant fields shown in the display.

Table 167: show ipv6 rpf Field Descriptions

Field	Description
RPF information for 2001::1:1:2	Source address that this information concerns.
RPF interface:Ethernet3/2	For the given source, the interface from which the router expects to get packets.
RPF neighbor:FE80::40:1:3	For the given source, the neighbor from which the router expects to get packets.
RPF route/mask:20::/64	Route number and mask that matched against this source.
RPF type:Unicast	Routing table from which this route was obtained, either unicast, multiprotocol BGP, or static mroutes.
RPF recursion count	Indicates the number of times the route is recursively resolved.
Metric preference:110	The preference value used for selecting the unicast routing metric to the Route Processor (RP) announced by the designated forwarder (DF).
Metric:30	Unicast routing metric to the RP announced by the DF.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) Inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

The table below describes the significant fields shown in the display.

Table 168: show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters**command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters {**interface** *type number* | **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays first-hop packets that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 snooping counters** command displays packets handled by the switch that are being counted in interface counters. The switch counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on Fast Ethernet interface 4/12:

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0
Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

The table below describes the significant fields shown in the display.

Table 169: show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from:	Bridged messages from the interface.
Dropped messages on:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:	The reason that these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **show ipv6 snooping features** command displays the first-hop features that are configured on the router.

Examples

The following example shows that both IPv6 NDP inspection and IPv6 RA guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

The table below describes the significant fields shown in the display.

Table 170: show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
priority	The priority of the specified feature.
state	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command in user EXEC or privileged EXEC mode.

show ipv6 snooping policies {**interface** *type number* | **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays policies that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **show ipv6 snooping policies** command displays all policies that are configured and lists the interfaces to which they are attached.

Examples

The following example shows information about all policies configured:

```
Device# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

The table below describes the significant fields shown in the display.

Table 171: show ipv6 snooping policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show ipv6 source-guard policy

To display the IPv6 source-guard policy configuration, use the **show ipv6 source-guard policy** command in user EXEC or privileged EXEC mode.

show ipv6 source-guard policy [*source-guard-policy*]

Syntax Description

source-guard-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco Release 15.3(1)S.

Usage Guidelines

The **show ipv6 source-guard policy** command displays the IPv6 source-guard policy configuration, as well as all the interfaces on which the policy is applied. The command also displays IPv6 prefix guard information if the IPv6 prefix guard feature is enabled on the device.

Examples

```
Device# show ipv6 source-guard policy policy1

Policy policy1 configuration:
data-glean
prefix-guard
address-guard

Policy policy1 is applied on the following targets:
Target           Type  Policy               Feature        Target range
Et0/0            PORT   policy1             source-guard   vlan all
vlan 100         VLAN   policy1             source-guard   vlan all
```

Related Commands

Command	Description
ipv6 source-guard attach-policy	Applies IPv6 source guard on an interface.
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

show ipv6 spd

To display the IPv6 Selective Packet Discard (SPD) configuration, use the **show ipv6 spd**command in privileged EXEC mode.

show ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **show ipv6 spd** command to display the SPD configuration, which may provide useful troubleshooting information.

Examples

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

```
Router# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

The table below describes the significant fields shown in the display.

Table 172: show ipv6 spd Field Description

Field	Description
Current mode: normal	The current SPD state or mode.
Queue max threshold: 74	The process input queue maximum.

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.

show ipv6 static

To display the current contents of the IPv6 routing table, use the **show ipv6 static** command in user EXEC or privileged EXEC mode.

show ipv6 static [{*ipv6-address* | *ipv6-prefix* / *prefix-length*}] [{**interface** *type number* | **recursive**}] [**detail**]

Syntax Description

ipv6-address	(Optional) Provides routing information for a specific IPv6 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.
ipv6-prefix	(Optional) Provides routing information for a specific IPv6 network. 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	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
interface	(Optional) Name of an interface.
type	(Optional, but required if the **interface** keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function.
number	(Optional, but required if the **interface** keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function.
recursive	(Optional) Allows the display of recursive static routes only.
detail	(Optional) Specifies the following additional information: • For valid recursive routes, the output path set and maximum resolution depth. • For invalid recursive routes, the reason why the route is not valid. • For invalid direct or fully specified routes, the reason why the route is not valid.

Command Default

All IPv6 routing information for all active routing tables is displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1.0	This command was modified. It was integrated into Cisco IOS XE Release 2.1.0.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.

Usage Guidelines

The **show ipv6 static** command provides output similar to the **show ip route** command, except that it is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the *type number* arguments are specified, only the specified interface-specific routes are displayed.

Examples

show ipv6 static Command with No Options Specified in the Command Syntax: Example

When no options specified in the command, those routes installed in the IPv6 Routing Information Base (RIB) are marked with an asterisk, as shown in the following example:

```
Router# show ipv6 static

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

The table below describes the significant fields shown in the display.

Table 173: show ipv6 static Field Descriptions

Field	Description
via nexthop	Specifies the address of the next router in the path to the remote network.
distance 1	Indicates the administrative distance to the specified route.

show ipv6 static Command with the IPv6 Address and Prefix: Example

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only information about static routes for that address or network is displayed. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
Router# show ipv6 static 2001:200::/35

IPv6 Static routes
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1
```

show ipv6 static interface Command: Example

When an interface is supplied, only those static routes with the specified interface as the outgoing interface are displayed. The **interface** keyword may be used with or without the IPv6 address and prefix specified in the command statement.

```
Router# show ipv6 static interface ethernet 3/0
```

IPv6 Static routes Code: * - installed in RIB 5000::/16, interface Ethernet3/0, distance 1

show ipv6 static recursive Command: Example

When the **recursive** keyword is specified, only recursive static routes are displayed:

```
Router# show ipv6 static recursive
```

IPv6 Static routes Code: * - installed in RIB * 4000::/16, via nexthop 2001:1::1, distance 1 * 5555::/16, via nexthop 4000::1, distance 1 5555::/16, via nexthop 9999::1, distance 1

show ipv6 static detail Command: Example

When the **detail** keyword is specified, the following additional information is displayed:

- For valid recursive routes, the output path set and maximum resolution depth.
- For invalid recursive routes, the reason why the route is not valid.
- For invalid direct or fully specified routes, the reason why the route is not valid.

```
Router# show ipv6 static detail

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
     Resolves to 1 paths (max depth 1)
     via Ethernet1/0
```

```
  5000::/16, interface Ethernet3/0, distance 1
     Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
     Resolves to 1 paths (max depth 2)
     via Ethernet1/0
  5555::/16, via nexthop 9999::1, distance 1
     Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ip route	Displays the current state of the routing table.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic**command in user EXEC or privileged EXEC mode.

show ipv6 traffic [**interface** [*interface type number*]]

Syntax Description

interface	(Optional) All interfaces. IPv6 forwarding statistics for all interfaces on which IPv6 forwarding statistics are being kept will be displayed.
interface type number	(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The *interface* argument and **interface** keyword were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

Examples

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

```
Device# 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 not a device
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation 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 info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 device solicit, 0 device advert, 0 redirects
```

The following is sample output for the show ipv6 interface command without IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

The following is sample output for the show ipv6 interface command with IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
```

```
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised 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.
```

The table below describes the significant fields shown in the display.

Table 174: show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
truncated	Number of truncated packets.
format errors	Errors that can result from checks performed on header fields, the version number, and packet length.
not a device	Message sent when IPv6 unicast routing is not enabled.
0 unicast RPF drop, 0 suppressed RPF drop	Number of unicast and suppressed reverse path forwarding (RPF) drops.
failed	Number of failed fragment transmissions.
encapsulation failed	Failure that can result from an unresolved address or try-and-queue packet.
no route	Counted when the software discards a datagram it did not know how to route.

Field	Description
unreach	Unreachable messages received are as follows: • routing--Indicates no route to the destination. • admin--Indicates that communication with the destination is administratively prohibited. • neighbor--Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source. • address--Indicates that the address is unreachable. • port--Indicates that the port is unreachable.
Unicast RPF access-list MINI	Unicast RPF access-list in use.
Process Switching	Displays process RPF counts, such as verification and suppressed verification drops.
CEF Switching	Displays CEF switching counts, such as verification drops and suppressed verification drops.

show ipv6 tunnel

To display IPv6 tunnel information, use the **show ipv6 tunnel**command in user EXEC or privileged EXEC mode.

show ipv6 tunnel

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

For each tunnel running IPv6, use the **show ipv6 tunnel** command to display the tunnel unit number, the name of the dynamic routing protocol used by the tunnel, the time of last input, the number of packets in the last input, and the description string as set by the **description** command.

Examples

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

```
Router# show ipv6 tunnel
Tun Route  LastInp  Packets
  0 RIPng    never        0
  1   -   00:00:13    55495
  2   -      never        0
  3   -   00:00:21    14755
  4   -      never        0
  5   -   00:00:00    15840
  6   -      never        0
  7   -   00:00:18    16008
  8   -      never        0
  9   -      never        0
 10   -      never        0
 11   -   00:00:03    94801
 12   -      1d02h        2
```

```
13   -      never        0
14   -   00:00:08   312190
15   -      never        0
16   -      never        0
17   -      never        0
18   -   00:00:05  1034954
19   -      never        0
20   -   00:00:01  1171114
21   -      never        0
```

The table below describes the significant fields shown in the display.

Table 175: show ipv6 tunnel Field Descriptions

Field	Description
Tun	Tunnel number.
Route	Indicates whether IPv6 RIP is enabled (RIPng) on this tunnel interface or is not enabled (-).
Last Inp	Time of last input into the tunnel.
Packets	Number of packets in this tunnel.
Description (not shown in sample output)	Description of the tunnel as entered in interface configuration mode.

show ipv6 virtual-reassembly

To display Virtual Fragment Reassembly (VFR) configuration and statistical information on a specific interface, use the **show ipv6 virtual-reassembly** command in privileged EXEC mode.

show ipv6 virtual-reassembly interface *interface-type*

Syntax Description

interface *interface-type*	Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on the given interface.

Examples

The following example shows a typical display produced by this command:

```
Router# show ipv6 virtual-reassembly
All enabled IPv6 interfaces...
GigabitEthernet0/0/0:
   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 64
   IPv6 configured fragments per reassembly (max-fragments): 16
   IPv6 configured reassembly timeout (timeout): 3 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:20
   IPv6 total reassembly timeout count:0
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.

show ipv6 virtual-reassembly features

To display Virtual Fragment Reassembly (VFR) information on all interfaces or on a specified interface, use the **show ipv6 virtual-reassembly features** command in privileged EXEC mode.

show ipv6 virtual-reassembly features [**interface** *interface-type*]

Syntax Description

interface *interface-type*	(Optional) Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on a specified interface or on all interfaces. Use the optional **interface** *interface-type* keyword and argument to specify an interface. If you enter the **show ipv6 virtual-reassembly features** command without the keyword and argument, information about all interfaces is displayed.

Examples

The following example displays information about all interfaces:

```
Router# show ipv6 virtual-reassembly features

GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [in]
  Features to use if IPV6 VFR is Enabled:CLI
GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [out]
  Features to use if IPV6 VFR is Enabled:CLI
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.
show ipv6 virtual-reassembly	Displays VFR configuration and statistical information.

show ipv6 wccp

To display the IPv6 Web Cache Communication Protocol (WCCP) global configuration and statistics, use the **show ipv6 wccp** command in user EXEC or privileged EXEC mode.

`show ipv6 wccp [[all] [capabilities] [summary] [ interfaces[{cef|counts| detail}] ][vrf` *vrf-name*`][{web-cache`*service-number*`}[[assignment] [clients] [counters] [detail] [service] [view]]]]`

Syntax Description

summary	(Optional) Displays a summary of WCCP services.
capabilities	(Optional) Displays WCCP platform capabilities information.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance associated with a service group to display.
service-number	(Optional) Identification number of the web cache service group being controlled by the cache. The number can be from 0 to 254. For web caches using Cisco cache engines, the reverse proxy service is indicated by a value of 99.
interfaces	(Optional) Displays WCCP redirect interfaces.
cef	(Optional) Displays Cisco Express Forwarding interface statistics, including the number of input, output, dynamic, static, and multicast services.
counts	(Optional) Displays WCCP interface count statistics, including the number of Cisco Express Forwarding and process-switched output and input packets redirected.
detail	(Optional) Displays WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
web-cache	(Optional) Displays statistics for the web cache service.
all	(Optional) Displays statistics for all known services.
assignment	(Optional) Displays service group assignment information.
service	(Optional) Displays detailed information about a service, including the service definition and all other per-service information.
clients	(Optional) Displays detailed information about the clients of a service, including all per-client information. No per-service information is displayed.
detail	(Optional) Displays detailed information about the clients of a service, including all per-client information. No per-service information is displayed. Assignment information is also displayed.
counters	(Optional) Displays traffic counters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Use the **clear ipv6 wccp** command to reset all WCCP counters.

Use the **show ipv6 wccp** *service-number* **detail** command to display information about the WCCP client timeout interval and the redirect assignment timeout interval if those intervals are not set to their default value of 10 seconds.

Use the **show ipv6 wccp summary** command to show the configured WCCP services and a summary of their current state.

Examples

This section contains examples and field descriptions for the following forms of this command:

- **show ipv6 wccp** *service-number* (service mode displayed)
- **show ipv6 wccp** *service-number* **detail**
- **show ipv6 wccp interfaces**
- **show ipv6 wccp web-cache**
- **show ipv6 wccp web-cache counters**
- **show ipv6 wccp web-cache detail**
- **show ipv6 wccp web-cache detail** (bypass counters displayed)
- **show ipv6 wccp web-cache service**
- **show ipv6 wccp summary**

show ipv6 wccp *service-number* (Service Mode Displayed)

The following is sample output from the **show ipv6 wccp** *service-number* command:

```
Router# show ipv6 wccp 61

Global WCCP information:
    Router information:
        Router Identifier:                   2001:DB8:100::1

    Service Identifier: 61
        Protocol Version:                    2.01
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        Total Packets Dropped Closed:        0
        Redirect access-list:                -none-
        Total Packets Denied Redirect:       0
```

```
Total Packets Unassigned:            0
Group access-list:                   -none-
Total Messages Denied to Group:      0
Total Authentication failures:       0
Total GRE Bypassed Packets Received: 0
  Process:                           0
  CEF:                               0
```

The table below describes the significant fields shown in the display.

Table 176: show ipv6 wccp service-number Field Descriptions

Field	Description
Router information	A list of routers detected by the current router.
Protocol Version	The version of WCCP being used by the router in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	The number of clients that are visible to the router and other clients in the service group.
Number of Service Group Routers	The number of routers in the service group.
Total Packets s/w Redirected	Total number of packets redirected by the router.
Service mode	Identifies the WCCP service mode. Options are Open or Closed.
Service Access-list	A named extended IP access list that defines the packets that will match the service.
Total Packets Dropped Closed	Total number of packets that were dropped when WCCP is configured for closed services and an intermediary device is not available to process the service.
Redirect Access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group Access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.
Total Bypassed Packets Received	The number of packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

show ipv6 wccp *service-number* detail

The following example displays WCCP client information and WCCP router statistics that include the type of services:

```
Router# show ipv6 wccp 61 detail

WCCP Client information:
        WCCP Client ID:          2001:DB8:1::11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             L2
        Packet Return:           L2
        Assignment:              MASK
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          32 of 64 (50.00%)
        Assigned masks/values:   1/32

        Mask  SrcAddr    DstAddr    SrcPort DstPort
        ----  -------    -------    ------- -------
        0000: ::3        ::F        0x0000  0x0000

        Value SrcAddr    DstAddr    SrcPort DstPort
        ----- -------    -------    ------- -------
        0000: ::         ::         0x0000  0x0000
        0001: ::         ::2        0x0000  0x0000
        0002: ::         ::4        0x0000  0x0000
        0003: ::         ::6        0x0000  0x0000
        0004: ::         ::8        0x0000  0x0000
        0005: ::         ::A        0x0000  0x0000
        0006: ::         ::C        0x0000  0x0000
        0007: ::         ::E        0x0000  0x0000
        0008: ::1        ::         0x0000  0x0000
        0009: ::1        ::2        0x0000  0x0000
        0010: ::1        ::4        0x0000  0x0000
        0011: ::1        ::6        0x0000  0x0000
        0012: ::1        ::8        0x0000  0x0000
        0013: ::1        ::A        0x0000  0x0000
        0014: ::1        ::C        0x0000  0x0000
        0015: ::1        ::E        0x0000  0x0000
        0016: ::2        ::         0x0000  0x0000
        0017: ::2        ::2        0x0000  0x0000
        0018: ::2        ::4        0x0000  0x0000
        0019: ::2        ::6        0x0000  0x0000
        0020: ::2        ::8        0x0000  0x0000
        0021: ::2        ::A        0x0000  0x0000
        0022: ::2        ::C        0x0000  0x0000
        0023: ::2        ::E        0x0000  0x0000
        0024: ::3        ::         0x0000  0x0000
        0025: ::3        ::2        0x0000  0x0000
        0026: ::3        ::4        0x0000  0x0000
        0027: ::3        ::6        0x0000  0x0000
        0028: ::3        ::8        0x0000  0x0000
        0029: ::3        ::A        0x0000  0x0000
        0030: ::3        ::C        0x0000  0x0000
        0031: ::3        ::E        0x0000  0x0000
```

```
WCCP Client ID:          2001:DB8:1::12
Protocol Version:        2.01
State:                   Usable
Redirection:             L2
Packet Return:           L2
Assignment:              MASK
Connect Time:            1w0d
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Mask Allotment:          32 of 64 (50.00%)
Assigned masks/values:   1/32

Mask  SrcAddr    DstAddr    SrcPort DstPort
----  -------    -------    ------- -------
0000: ::3        ::F        0x0000  0x0000

Value SrcAddr    DstAddr    SrcPort DstPort
----- -------    -------    ------- -------
0000: ::         ::1        0x0000  0x0000
0001: ::         ::3        0x0000  0x0000
0002: ::         ::5        0x0000  0x0000
0003: ::         ::7        0x0000  0x0000
0004: ::         ::9        0x0000  0x0000
0005: ::         ::B        0x0000  0x0000
0006: ::         ::D        0x0000  0x0000
0007: ::         ::F        0x0000  0x0000
0008: ::1        ::1        0x0000  0x0000
0009: ::1        ::3        0x0000  0x0000
0010: ::1        ::5        0x0000  0x0000
0011: ::1        ::7        0x0000  0x0000
0012: ::1        ::9        0x0000  0x0000
0013: ::1        ::B        0x0000  0x0000
0014: ::1        ::D        0x0000  0x0000
0015: ::1        ::F        0x0000  0x0000
0016: ::2        ::1        0x0000  0x0000
0017: ::2        ::3        0x0000  0x0000
0018: ::2        ::5        0x0000  0x0000
0019: ::2        ::7        0x0000  0x0000
0020: ::2        ::9        0x0000  0x0000
0021: ::2        ::B        0x0000  0x0000
0022: ::2        ::D        0x0000  0x0000
0023: ::2        ::F        0x0000  0x0000
0024: ::3        ::1        0x0000  0x0000
0025: ::3        ::3        0x0000  0x0000
0026: ::3        ::5        0x0000  0x0000
0027: ::3        ::7        0x0000  0x0000
0028: ::3        ::9        0x0000  0x0000
0029: ::3        ::B        0x0000  0x0000
0030: ::3        ::D        0x0000  0x0000
0031: ::3        ::F        0x0000  0x0000
```

Table 177: show ipv6 wccp service-number detail Field Descriptions

Field	Description
Protocol Version	The version of WCCP being used by the router in the service group.

Field	Description
State	Indicates whether the WCCP client is operating properly and can be contacted by a router and other clients in the service group. When a WCCP client has an incompatible message interval setting, the state of the client is shown as "NOT Usable," followed by a status message describing the reason why the client is not usable.
Redirection	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Assignment	Indicates the load-balancing method used. WCCP uses HASH or MASK assignment.
Message Interval	The fixed time interval (in seconds)between successive keepalive messages sent from a WCCCP client to a WCCP router. The default time interval is 10 seconds. If the default time interval is configured, the "Message Interval" field is not displayed.
Client timeout	The time (in seconds) that must pass without a WCCP router receiving a keepalive message from a client before the WCCP router considers that client unreachable and removes it from the service group.
Assignment timeout	The time (in seconds) that must pass after the WCCP router detects a failed client and begins to redirect traffic.
Packets Redirected	The number of packets that have been redirected to the content engine.
Connect Time	The amount of time (in hours, minutes, and seconds) the client has been connected to the router.

show ipv6 wccp interfaces

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

```
Router# show ipv6 wccp interfaces

WCCP interface configuration:
    FastEthernet0/1/0
        Output services: 2
        Input services: 3
        Mcast services: 1
        Exclude In:      FALSE
```

The table below describes the significant fields shown in the display.

Table 178: show ipv6 wccp interfaces Field Descriptions

Field	Description
Output services	Indicates the number of output services configured on the interface.
Input services	Indicates the number of input services configured on the interface.
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

show ipv6 wccp web-cache

The following is sample output from the **show ipv6 wccp web-cache** command:

```
Router# show ipv6 wccp web-cache

Global WCCP information:
    Router information:
        Router Identifier:                   2001:DB8:100::1

    Service Identifier: web-cache
        Protocol Version:                    2.01
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        Total Packets Dropped Closed:        0
        Redirect access-list:                -none-
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
        GRE tunnel interface:                Tunnel1
```

The table below describes the significant fields shown in the display.

Table 179: show ipv6 wccp web-cache Field Descriptions

Field	Description
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	Number of clients using the router as their home router.
Number of Service Group Routers	The number of routers in the service group.
Total Packets Redirected	Total number of packets redirected by the router.
Service mode	Indicates whether WCCP open or closed mode is configured.
Service Access-list	The name or number of the service access list that determines which packets will be redirected.
Redirect access-list	The name or number of the access list that determines which packets will be redirected.

Field	Description
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.

show ipv6 wccp web-cache counters

The following example displays web cache engine information and WCCP traffic counters:

```
Router# show ipv6 wccp web-cache counters

WCCP Service Group Counters:
   Redirected Packets:
     Process:                   0
     CEF:                       0
   Non-Redirected Packets:
     Action - Forward:
       Reason - no assignment:
         Process:               0
         CEF:                   0
     Action - Ignore (forward):
       Reason - redir ACL check:
         Process:               0
         CEF:                   0
     Action - Discard:
       Reason - closed services:
         Process:               0
         CEF:                   0
   GRE Bypassed Packets:
     Process:                   0
     CEF:                       0
   GRE Bypassed Packet Errors:
     Total Errors:
       Process:                 0
       CEF:                     0

   WCCP Client Counters:
     WCCP Client ID:            2001:DB8:1::11
       Redirect Assignments:
         Received:              1
         Invalid:               0
         Duplicate:             0
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
```

```
     WCCP Client ID:             2001:DB8:1::12
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
```

The table below describes the significant fields shown in the display.

Table 180: show ipv6 wccp web-cache counters Field Descriptions

Field	Description
Redirected Packets	Total number of packets redirected by the router.
Non-Redirected Packets	Total number of packets not redirected by the router.

show ipv6 wccp web-cache detail

The following example displays web cache engine information and WCCP router statistics for the web cache service:

```
Router# show ipv6 wccp web-cache detail

WCCP Client information:
        WCCP Client ID:          2001:DB8:1::11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Hash Allotment:          128 of 256 (50.00%)
        Initial Hash Info:       00000000000000000000000000000000
                                 00000000000000000000000000000000
        Assigned Hash Info:      55555555555555555555555555555555
                                 55555555555555555555555555555555

        WCCP Client ID:          2001:DB8:1::12
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
```

```
    CEF:                     0
  Hash Allotment:          128 of 256 (50.00%)
  Initial Hash Info:       00000000000000000000000000000000
                           00000000000000000000000000000000
  Assigned Hash Info:      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                           AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

The table below describes the significant fields shown in the display.

Table 181: show ipv6 wccp web-cache detail Field Descriptions

Field	Description
WCCP Client Information	The header for the area that contains fields for information on clients.
IP Address	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Redirected Packets	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time (in hours, minutes, and seconds) the cache engine has been connected to the router.

show ipv6 wccp web-cache detail (Bypass Counters)

The following example displays web cache engine information and WCCP router statistics that include the bypass counters:

```
Router# show ipv6 wccp web-cache detail

WCCP Client information:
        WCCP Client ID:          2001:DB8:1::11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Hash Allotment:          128 of 256 (50.00%)
        Initial Hash Info:       00000000000000000000000000000000
                                 00000000000000000000000000000000
        Assigned Hash Info:      55555555555555555555555555555555
                                 55555555555555555555555555555555

        WCCP Client ID:          2001:DB8:1::12
        Protocol Version:        2.01
        State:                   Usable
```

```
Redirection:             GRE
Packet Return:           GRE
Assignment:              HASH
Connect Time:            1w0d
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Hash Allotment:          128 of 256 (50.00%)
Initial Hash Info:       00000000000000000000000000000000
                         00000000000000000000000000000000
Assigned Hash Info:      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                         AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

The table below describes the significant fields shown in the display.

Table 182: show ipv6 wccp web-cache detail Field Descriptions

Field	Description
WCCP Router information	The header for the area that contains fields for the IP address and the version of WCCP associated with the router connected to the cache engine in the service group.
IP Address	The IP address of the router connected to the cache engine in the service group.
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
WCCP Client Information	The header for the area that contains fields for information on clients.
IP Address	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Initial Hash Info	The initial state of the hash bucket assignment.
Assigned Hash Info	The current state of the hash bucket assignment.
Hash Allotment	The percent of buckets assigned to the current cache engine. Both a value and a percent figure are displayed.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time (in hours, minutes, and seconds) the cache engine has been connected to the router.
Bypassed Packets	The number of packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

show ipv6 wccp web-cache service

The following example displays information about a service, including the service definition and all other per-service information:

```
Router# show ipv6 wccp web-cache service

WCCP service information definition:
        Type:          Standard
        Id:            0
        Priority:      240
        Protocol:      6
        Options:       0x00000512
        --------
            Mask/Value sets: 1
            Value elements: 4
            Dst Ports: 80 0 0 0 0 0 0 0
```

show ipv6 wccp summary

The following example displays information on the configured WCCP services and a summary of their current state:

```
Router# show ipv6 wccp summary

WCCP version 2 enabled, 2 services
Service     Clients   Routers   Assign      Redirect   Bypass
-------     -------   -------   ------      --------   ------
Default routing table (Router Id: 2001:DB8:100::1):
web-cache   2         1         HASH        GRE        GRE
61          2         1         MASK        L2         L2
62          2         1         MASK        L2         L2
```

The table below describes the significant fields shown in the display.

Table 183: show ipv6 wccp summary Field Descriptions

Field	Description
Service	Indicates which service is detailed.
Clients	Indicates the number of cache engines participating in the WCCP service.
Routers	Indicates the number of routers participating in the WCCP service.
Assign	Indicates the load-balancing method used. WCCP uses HASH or MASK assignment.
Redirect	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Bypass	Indicates the bypass method used. WCCP uses GRE or L2 to return packets to the router.

Related Commands

Command	Description
clear ipv6 wccp	Clears the counter for packets redirected using WCCP.

Command	Description
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
show ipv6 interface	Lists a summary of the IP information and status of an interface.
show ipv6 wccp global counters	Displays global WCCP information for packets that are processed in software.

show ipv6 wccp global counters

To display IPv6 global Web Cache Communication Protocol (WCCP) information for packets that are processed in software, use the **show ipv6 wccp global counters** command in user EXEC or privileged EXEC mode.

show ipv6 wccp global counters

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

The **show ipv6 wccp globalcounters** command displays counters for packets that are processed in software.

Examples

The following example displays global WCCP information for packets that are processed in the software:

```
Router# show ipv6 wccp global counters

WCCP Global Counters:
Packets Seen by WCCP
Process:   8
CEF (In):  14
CEF (Out): 0
```

The table below describes the significant fields shown in the display.

Table 184: show ipv6 wccp global counters Field Descriptions

Field	Description
CEF (In)	Number of incoming Cisco Express Forwarding packets
CEF (Out)	Number of outgoing Cisco Express Forwarding packets.

Related Commands

Command	Description
clear ipv6 wccp	Clears the counters for packets redirected using WCCP.
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.

Command	Description
show ipv6 interface	Lists a summary of the IP information and the status of an interface.
show ipv6 wccp	Displays the WCCP global configuration and statistics.

show isis ipv6 rib

To display the Intermediate System-to-Intermediate System (IS-IS) IPv6 local routing information base (RIB), use the **show isis ipv6 rib** command in user EXEC or privileged EXEC mode.

show isis ipv6 rib [*ipv6-prefix*]
no show isis ipv6 rib [*ipv6-prefix*]

Syntax Description

ipv6-prefix	(Optional) IPv6 address prefix. This argument must be in the form documented in RFC 2373 with the address specified in hexadecimal, 16-bit values between colons.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series devices.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(3)M	This command was modified. Filtered routes are now represented by a hyphen (-).

Usage Guidelines

When the optional *ipv6-prefix* argument is not used, the complete Intermediate System-to-Intermediate System (IS-IS) IPv6 RIB is displayed. When an optional IPv6 prefix is supplied, only the entry matching that prefix is displayed.

Only the optimal paths will be installed in the primary IPv6 RIB as IS-IS routes.

Examples

The following is sample output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed and a hyphen (-) indicates prefixes that have been filtered out in the primary IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Device# show isis ipv6 rib
```

```
IS-IS IPv6 process , local RIB
  11::1/128
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
  20::/64
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2]
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
* 22::2/128
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2] -
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3] -
  2001:DB8::/64
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2]
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
```

The table below describes the significant fields shown in the display.

Table 185: show isis ipv6 rib Field Descriptions

Field	Description
11::1/128	IPv6 prefix that is stored within the IS-IS local RIB.
via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0	IPv6 address of the next hop—in this instance, Ethernet0/0.
type	Type of path: • L1—Level 1 • L2—Level 2
tag	Priority of the IPv6 prefix. All prefixes have a tag 0 priority unless otherwise configured.
LSP [3/3]	Link-state packet (LSP). The numbers following LSP indicate the LSP index and LSP version, respectively.
*	Prefixes that have been installed in the primary IPv6 RIB as IS-IS routes.
-	Route paths that are filtered out.

Related Commands

Command	Description
distribute-list in (IP)	Filters routes received in incoming updates.
show isis ip rib	Displays the IS-IS IPv4 local RIB.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

show monitor event-trace vpn-mapper

To display event trace messages for IPv6 virtual private networks (VPNs), use the **show monitor event-trace vpn-mapper**command in privileged EXEC mode.

show monitor event-trace vpn-mapper {**latest** | **all**}

Syntax Description

latest	Displays only the event trace messages since the last **show monitor event-trace** command was entered.
all	Displays all event trace messages currently in memory for the specified component.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show monitor event-trace** command to display trace message information about IPv6 VPNs.

Examples

The following example allows event trace messages for IPv6 VPNs to be displayed:

```
Router# show monitor event-trace vpn-mapper
```

show ospfv3 border-routers

To display the internal Open Shortest Path First version 3 (OSPFv3) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospfv3 border-routers** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}] **border-routers**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A VRF name of "*" displays information for all VRFs, including the global table.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
Cisco IOS Release 15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS Release 15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following examples enables the display of the internal OSPFv3 routing table entries to an ABR and ASBR:

```
Router# show ospfv3 border-routers
```

show ospfv3 database

To display lists of information related to the Open Shortest Path First version 3 (OSPFv3) database for a specific router, use the **show ospfv3 database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPFv3 link-state advertisements (LSAs).

{**show ospfv3** [*process-id* [*area-id*]] [*address-family*] [**vrf** {*vrf-name* | *****}]**database** [{**database-summary** | **internal** | **external** [**ipv6-prefix**] [*link-state-id*]}] | **grace** | **inter-area prefix** [{**ipv6-prefix***link-state-id*}] | **inter-area router** [{**destination-router-id***link-state-id*}] | **link** [{**interface** *interface-namelink-state-id*}] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [{**ref-lsa** {**router** | **network**}*link-state-id*}] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**]}

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area. The *area-id* argument can only be used if the *process-id* argument is specified.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
database-summary	(Optional) Displays how many of each type of LSAs exist for each area in the database, and the total.
internal	(Optional) Internal LSA information.
external	(Optional) Displays information only about the external LSAs.
ipv6-prefix	(Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
grace	(Optional) Displays information about OSPFv3 graceful restart.
link-state-id	(Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.

destination-router-id	(Optional) The specified destination router ID.
link	(Optional) Displays information about the link LSAs.
interface	(Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information on the intra-area-prefix LSAs.
promiscuous	(Optional) Displays temporary LSAs in a Mobile Ad Hoc Network (MANET).
ref-lsa {**router** | **network**}	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays all LSAs with unknown types.
area	(Optional) Filters unknown area LSAs.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
link	(Optional) When following the **unknown** keyword, the **link** keyword filters link-scope LSAs.
adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ospfv3 database**database command to provide more detailed information.

Examples

The following is sample output from the **show ospfv3 database** command when no arguments or keywords are used:

```
Router# show ospfv3 database
            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)
                Router Link States (Area 0)
ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Router Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
            Intra Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

The table below describes the significant fields shown in the display.

Table 186: show ospfv3 database Field Descriptions

Field	Description
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Link ID	Interface ID number.
Ref-lstype	Referenced link-state type.
Ref-LSID	Referenced link-state ID.

show ospfv3 events

To display detailed information about Open Shortest Path First version 3 (OSPFv3) events, use the **show ospfv3 events**command in privileged EXEC mode.

show **ospfv3** [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**events** [{**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**}]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
generic	(Optional) Generic information regarding OSPFv3 events.
interface	(Optional) Interface state change events, including old and new states.
lsa	(Optional) LSA arrival and LSA generation events.
neighbor	(Optional) Neighbor state change events, including old and new states.
reverse	(Optional) Keyword to allow the display of events in reverse-from the latest to the oldest or from oldest to the latest.
rib	(Optional) Routing Information Base (RIB) update, delete, and redistribution events.
spf	(Optional) Scheduling and SPF run events.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

An OSPFv3 event log is kept for every OSPFv3 instance. If you enter the **show ospfv3 events** command without any keywords, all information in the OSPFv3 event log is displayed. Use the keywords to filter specific information.

Examples

The following example enables the display of information about OSPFv3 events:

```
Router# show ospfv3 events
```

show ospfv3 flood-list

To display a list of Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **s how ospfv3 flood-list**command in privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**flood-list** *interface-type* *interface-number*

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command to display OSPFv3 packet pacing.

Examples

The following displays a list of OSPFv3 LSAs waiting to be flooded over an interface:

```
Router# show ospfv3 flood-list
```

show ospfv3 graceful-restart

To display Open Shortest Path First version 3 (OSPFv3) graceful restart information, use the **show ospfv3 graceful-restart** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *}]**graceful-restart**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **show ospfv3 graceful-restart** command to discover information about the OSPFv3 graceful restart feature.

Examples

The following example displays OSPFv3 graceful restart information:

```
Router# show ospfv3 graceful-restart
```

show ospfv3 interface

To display Open Shortest Path First version 3 (OSPFv3)-related interface information, use the **show ospfv3 interface** command in privileged mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**interface** [*type number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information about a specified area only.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following is sample output from the **show ospfv3 interface** command for a Mobile Ad Hoc Network (MANET) environment:

```
Router# show ospfv3 interface
Ethernet0/0 is up, line protocol is up
Link Local Address FE80::A8BB:CCFF:FE01:5500, Interface ID 3
```

```
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3
Network Type MANET, Cost: 10 (dynamic), Cost Hysteresis: Disabled
Cost Weights: Throughput 100, Resources 100, Latency 100, L2-factor 100
Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
Incremental Hello is enabled
Local SCS number 1
Relaying enabled
Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
Router#
```

The table below describes the significant fields shown in the display.

Table 187: show ospfv3 interface Field Descriptions

Field	Description
Ethernet0/0	Status of the physical link and the operational status of the protocol.
Link Local Address	Interface IPv6 address.
Area 0, Process ID 100, Instance ID 0, Router ID 172.16.3.3	Area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type MANET, Cost: 10 (dynamic), Cost hysteresis: Disabled	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Timer intervals configured	Configuration of timer intervals, including hello-increment and dead-interval.
Hello due in 00:00:01	Number of seconds until the next hello packet is sent from this interface.
Supports Link-local Signaling (LLS)	Indicates that LLS is supported.
Last flood scan length is 2, maximum is 2	Indicates length of last flood scan and the maximum length.
Last flood scan time is 0 msec, maximum is 0 msec	Indicates how many milliseconds the last flood scan occurred and the maximum time length.
Neighbor Count	Count of network neighbors and a list of adjacent neighbors.

Field	Description
Adjacent with neighbor 2.2.2.2	Lists the adjacent neighbor.
Suppress hello for 0 neighbor(s)	Indicates the number of neighbors to suppress hello messages

show ospfv3 max-metric

To display Open Shortest Path First version 3 (OSPFv3) maximum metric origination information, use the **show ospfv3 max-metric** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**max-metric**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 max-metric** command is useful in debugging OSPFv3 routing operations. You can also use the **show ipv6 ospf max-metric** command display the same information as the **show ospfv3 max-metric** command.

Examples

The following is sample output from the **show ospfv3 max-metric** command:

```
Router# show ospfv3 1 max-metric
Routing Process "ospfv3 1" with ID 192.168.2.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Originating router-LSAs with maximum metric, Time remaining: 00:01:18
    Condition: on startup while BGP is converging, State: active
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

```
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
   Area BACKBONE(0)
       Number of interfaces in this area is 1
       SPF algorithm executed 2 times
       Number of LSA 6. Checksum Sum 0x0327C7
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

The table below describes the significant fields shown in the display.

Table 188: show ospfv3 max-metric command

Field	Description
Routing Process "ospfv3 1" with ID 192.168.2.1	The routing process specified by process ID.
Event-log enabled, Maximum number of events: 1000, Mode: cyclic	Configuration for this OSPFv3 process.
Originating router-LSAs with maximum metric, Time remaining: 00:01:18	
Condition: on startup while BGP is converging, State: active	The router advertises a max metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired.

show ospfv3 neighbor

To display Open Shortest Path First for IPv6 (OSPFv3) neighbor information on a per-interface basis, use the s**how ospfv3 neighbor** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name* | *****}] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**] [**summary** [**per-instance**]]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
interface-type interface-number	(Optional) Interface type and number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors in detail (lists all neighbors).
summary	(Optional) Displays total number summary of all neighbors.
per-instance	(Optional) Displays total number of neighbors in each neighbor state. The output is printed for each configured OSPF instance separately.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Release	Modification
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M. This command was modified. The **summary** and **per-instance** keywords were added.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S. This command was modified. The **summary** and **per-instance** keywords were added.

Examples

The following is sample output from the **show ospfv3 neighbor** command:

```
Device# show ospfv3 neighbor

OSPFv3 Router with ID (42.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
44.4.4.4        1    FULL/  -        00:00:39    12              vm1
OSPFv3 Router with ID (1.1.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
4.4.4.4          1    FULL/  -        00:00:35    12              vm1
```

The following is sample output from the **show ospfv3 neighbor** command with the **detail** keyword for a Mobile Ad Hoc Network (MANET) environment:

```
Device# show ospfv3 neighbor detail
Neighbor 42.4.4.4, interface address 4.4.4.4
In the process ID 42 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
Neighbor priority is 1, State is FULL, 6 state changes
Options is 0x000F12 in Hello (E-Bit, R-bit, AF-Bit, L-Bit, I-Bit, F-Bit)
Options is 0x000112 in DBD (E-Bit, R-bit, AF-Bit)
Dead timer due in 00:00:33
Neighbor is up for 00:09:43
Index 1/1/1, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor is incremental Hello capable
Last known SCS number 1
Neighbor's willingness 128
We are standby relay for the neighbor
This neighbor is standby relay for us
Neighbor is running Manet Version 10
Neighbor 4.4.4.4
In the process ID 100 area 0 via interface vmi1
Neighbor: interface-id 12, link-local address FE80::A8BB:CCFF:FE01:5800
Neighbor priority is 1, State is FULL, 6 state changes
Options is 0x000E13 in Hello (V6-Bit, E-Bit, R-bit, L-Bit, I-Bit, F-Bit)
Options is 0x000013 in DBD (V6-Bit, E-Bit, R-bit)
Dead timer due in 00:00:37
Neighbor is up for 00:09:43
Index 1/1/1, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor is incremental Hello capable
Last known SCS number 1
Neighbor's willingness 128
Two-hop neighbors:
5.5.5.5
```

```
We are standby relay for the neighbor
This neighbor is active relay for us
Neighbor is running Manet Version 10
Selective Peering is enabled
1 paths to this neighbor
Neighbor peering state: Slave, local peering state: Master,
Default cost metric is 0
Minimum incremental cost is 10
```

The table below describes the significant fields shown in the display.

Table 189: show ospfv3 neighbor Field Descriptions

Field	Description
Neighbor ID; Neighbor	Neighbor device ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
Pri; Neighbor priority	Device priority of the neighbor, neighbor state.
State	OSPFv3 state.
State changes	Number of state changes since the neighbor was created.
Options	Hello packet options field contents (E-bit only). Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer due in	Expected time before Cisco IOS software declares the neighbor dead.
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into two-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in the retransmission queue.
number of retransmission	Number of times update packets have been resent during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of link state advertisements (LSAs) in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

Field	Description
Neighbor is incremental Hello capable	The MANET neighbor interface is capable of receiving increment hello messages. A neighbor must be capable of sending and receiving incremental hello packets to be a full neighbor on a MANET interface.
Last known SCS number 1	Indicates the last received MANET state. The State Change Sequence number is included in the incremental hello packet.
Neighbor's willingness 128	Indicates the neighbors willingness to act as an active relay for this device, on a scale of 0 (not willing) to 255 (always willing). Willingness is used as a tiebreaker when electing an active relay.
We are standby relay for neighbor	Indicates that this device will not flood LSAs received from this neighbor until one or more of its neighbors fails to acknowledge receiving the LSA flood from another neighbor.
Neighbor is running Manet Version 10	Indicates the MANET version number. Devices cannot establish full adjacency unless they are running the same MANET version.
Two-hop neighbors	Lists the device IDs of all full neighbors of the specified device that are not also neighbors of this device.
Selective Peering is enabled	The MANET interface has selective peering enabled.
1 paths to this neighbor	Indicates the number of unique paths to this device that exist in the routing table. This number might exceed the redundancy level configured for this OSPFv3 process.
Neighbor peering state...	Indicates which device is entitled to make the selective peering decision. Generally speaking, the entitled device has the smaller number of full neighbors at the time the devices discover each other.
Default cost metric is 0	Indicates the maximum OSPFv3 cost to a new neighbor to be considered for selective peering. If 0, a threshold OSPFv3 cost is not required for consideration.
Minimum incremental cost is 10	Indicates the minimum cost increment for the specified interface.

The following is sample output from the **show ospfv3 neighbor summary** command:

```
Device# show ospfv3 neighbor summary

OSPFv3 1 address-family ipv6 (router-id 10.4.9.158)

DOWN          0
ATTEMPT       0
INIT          0
```

```
2WAY         0
EXSTART      0
EXCHANGE     0
LOADING      0
FULL         1
Total count  1    (Undergoing GR 0)
```

The following is sample output from the **show ospfv3 neighbor summary per-instance** command:

```
Device# show ospfv3 neighbor summary per-instance

OSPFv3 1 address-family ipv6 (router-id 10.4.9.158)

DOWN         0
ATTEMPT      0
INIT         0
2WAY         0
EXSTART      0
EXCHANGE     0
LOADING      0
FULL         1
Total count  0    (Undergoing GR 0)


Neighbor summary for selected OSPFv3 processes

DOWN         0
ATTEMPT      0
INIT         0
2WAY         0
EXSTART      0
EXCHANGE     0
LOADING      0
FULL         1
Total count  0    (Undergoing GR 0)
```

*Table 190: **show ospfv3 neighbor summary** and **show ospfv3 neighbor summary per-instance** Field Descriptions*

Field	Description
DOWN	No information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.
ATTEMPT	This state is only valid for manually configured neighbors in a Non-Broadcast Multi-Access (NBMA) environment. In Attempt state, the device sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.
INIT	This state specifies that the device has received a hello packet from its neighbor, but the receiving device's ID was not included in the hello packet. When a device receives a hello packet from a neighbor, it should list the sender's device ID in its hello packet as an acknowledgment that it received a valid hello packet.
2WAY	This state designates that bi-directional communication has been established between two devices.

Field	Description
EXSTART	This state is the first step in creating an adjacency between the two neighboring devices. The goal of this step is to decide which device is primary, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.
EXCHANGE	In this state, OSPF devices exchange database descriptor (DBD) packets. Database descriptors contain link-state advertisement (LSA) headers only and describe the contents of the entire link-state database. Each DBD packet has a sequence number which can be incremented only by the primary which is explicitly acknowledged by subordinate. Devices also send link-state request packets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the devices link-state database to check if new or more current link-state information is available with the neighbor.
LOADING	In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, devices send link-state request packets. The neighbor then provides the requested link-state information in link-state update packets. During the adjacency, if a device receives an outdated or missing LSA, it requests that LSA by sending a link-state request packet. All link-state update packets are acknowledged.
FULL	In this state, devices are fully adjacent with each other. All the device and network LSAs are exchanged and the devices' databases are fully synchronized. Full is the normal state for an OSPF device. If a device is stuck in another state, it's an indication that there are problems in forming adjacencies. The only exception to this is the 2-way state, which is normal in a broadcast network. Devices achieve the full state with their DR and BDR only. Neighbors always see each other as 2-way.

show ospfv3 request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ospfv3 request-list**command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 request-list** command is useful in debugging OSPFv3 routing operations.

Examples

The following example shows information about the LSAs requested by the router:

```
Router# show ospfv3 request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

The table below describes the significant fields shown in the display.

Table 191: show ospfv3 request-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ospfv3 retransmission-list**command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*area-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the Open Shortest Path First version 3 (OSPFv3) routing process and can be a value from 1 through 65535.
area-id	(Optional) Displays information only about a specified area.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.
interface neighbor	(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 retransmission-list** command is useful in debugging Open Shortest Path First version 3 (OSPFv3) routing operations.

Examples

The following is sample output from the **show ospfv3 retransmission-list** command:

```
Router# show ospfv3 retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

The table below describes the significant fields shown in the display.

Table 192: show ospfv3 retransmission-list Field Descriptions

Field	Description
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	Identification of the router for which information is displayed.
Interface Ethernet0/0	Interface for which information is displayed.
Link state retransmission due in	Length of time before next link-state transmission.
Queue length	Number of elements in the retransmission queue.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ospfv3 statistic

To display Open Shortest Path First version 3 (OSPFv3) shortest path first (SPF) calculation statistics, use the **show ospfv3 statistic** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**statistic** [**detail**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
detail	(Optional) Displays statistics separately for each OSPFv3 area and includes additional, more detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **show ospfv3 statistics** command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the **show ospfv3 statistics** command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following example provides detailed statistics for each OSPFv3 area:

```
Router# show ospfv3 statistics detail
  Area 0: SPF algorithm executed 3 times
SPF 1 executed 00:06:57 ago, SPF type Full
```

```
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/0(R)
SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
  Change record R L P
  LSAs changed 4
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

The table below describes the significant fields shown in the display.

Table 193: show ospfv3 statistics Field Descriptions

Field	Description
Area	OSPF area ID.
SPF	Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.
Executed ago	Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.
SPF type	SPF type can be Full or Incremental.
SPT	Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.
Ext	Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.
Total	Total duration time in milliseconds for the SPF algorithm process.

Field	Description
LSIDs processed	Number of LSAs processed during the SPF calculation: • N--Network LSA. • R--Router LSA. • SA--Summary Autonomous System Boundary Router (ASBR) (SA) LSA. • SN--Summary Network (SN) LSA. • Stub--Stub links. • X7--External Type-7 (X7) LSA.

show ospfv3 summary-prefix

To display a list of all summary address redistribution information configured under an Open Shortest Path First version 3 (OSPFv3) process, use the **show ospfv3 summary-prefix**command in user EXEC or privileged EXEC mode.

show **ospfv3** [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**summary-prefix**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Examples

The following is sample output from the **show ospfv3 summary-prefix** command:

```
Router# show ospfv3 summary-prefix

OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

The table below describes the significant fields shown in the display.

Table 194: show ospfv3 summary-prefix Field Descriptions

Field	Description
OSPFv3 Process	Process ID of the router for which information is displayed.
Metric	Metric used to reach the destination router.
Type	Type of link-state advertisement (LSA).
Tag	LSA tag.

show ospfv3 timers rate-limit

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the **show ospfv3 timers rate-limit**command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**timers rate-limit**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **show ospfv3 timers rate-limit** command to discover when LSAs in the queue will be sent.

Examples

The following is sample output from the **show ospfv3 timers rate-limit**command:

```
Router# show ospfv3 timers rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

The table below describes the significant fields shown in the display.

Table 195: show ospfv3 timers rate-limit Field Descriptions

Field	Description
LSAID	ID of the LSA.
Type	Type of LSA.
Adv Rtr	ID of the advertising router.
Due in:	When the LSA is scheduled to be sent (in hours:minutes:seconds).

show ospfv3 traffic

To display Open Shortest Path First version 3 (OSPFv3) traffic and neighbor statistics, use the **show ospfv3 traffic** command in privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**traffic** [*interface-type interface-number*]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.
interface-type interface-number	(Optional) Type and number associated with a specific OSPFv3 interface.

Command Default

When the **show ospfv3 traffic** command is entered without any arguments, global OSPFv3 traffic statistics are displayed, including queue statistics for each OSPFv3 process, statistics for each interface, and per OSPFv3 process statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can limit the displayed traffic statistics to those for a specific OSPFv3 process by entering a value for the *process-id* argument, or you can limit output to traffic statistics for a specific interface associated with an OSPFv3 process by entering values for the *interface-type* and *interface-number* arguments.

Examples

The following example shows the display output for the **show ospfv3 traffic** command for OSPFv3:

```
Router# show ospfv3 traffic
OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852
  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface Ethernet0/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960
  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
```

```
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   436
  RX DB des     7                    316
  RX LS req     2                    104
  RX LS upd     9                    692
  RX LS ack     4                    264
  RX Total      33                   1812
  TX Failed     0                    0
  TX Hello      19                   724
  TX DB des     12                   456
  TX LS req     2                    104
  TX LS upd     8                    628
  TX LS ack     6                    296
  TX Total      47                   2208
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

The table below describes the significant fields shown in the display.

Table 196: show ospfv3 traffic Field Descriptions

Field	Description
OSPFv3 statistics	Traffic statistics accumulated for all OSPFv3 processes running on the router. To ensure compatibility with the **show ip traffic** command, only checksum errors are displayed. Identifies the route map name.
OSPFv3 queues statistic for process ID	Queue statistics specific to Cisco IOS software.
Hello queue	Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPFv3 hello process for all received OSPFv3 packets.
Router queue	Statistics for the internal Cisco IOS queue between the OSPFv3 hello process and the OSPFv3 router for all received OSPFv3 packets except OSPFv3 hellos.
queue size	Actual size of the queue.
queue limit	Maximum allowed size of the queue.
queue max size	Maximum recorded size of the queue.
Interface statistics	Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.
OSPFv3 packets received/sent	Number of OSPFv3 packets received and sent on the interface, sorted by packet types.

Field	Description
OSPFv3 header errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.
OSPFv3 LSA errors	Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.
Summary traffic statistics for process ID	Summary traffic statistics accumulated for an OSPFv3 process. **Note** The OSPFv3 process ID is a unique value assigned to the OSPFv3 process in the configuration. The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPFv3 statistics.

show ospfv3 traffic neighbor

To display Open Shortest Path First version 3 (OSPFv3) traffic statistics per neighbor, use the **show ospfv3 traffic neighbor**command in user EXEC or privileged EXEC mode.

show ospfv3 traffic neighbor[*interface nbr-id*]

Syntax Description

interface nbr-id	(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.x	This command was introduced.

show ospfv3 virtual-links

To display parameters and the current state of Open Shortest Path First version 3 (OSPFv3) virtual links, use the **show ospfv3 virtual-links** command in user EXEC or privileged EXEC mode.

show ospfv3 [*process-id*] [*address-family*] [**vrf** {*vrf-name* | *****}]**virtual-links**

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
vrf	(Optional) VPN Routing/Forwarding instance.
{*vrf-name* | *****}	The virtual routing and forwarding table for which the information should be displayed. If this parameter is not specified, only information for the global routing table is shown. A vrf name of "*" displays information for all vrfs, including the global table.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The information displayed by the **show ospfv3 virtual-links** command is useful in debugging OSPFv3 routing operations.

Examples

The following is sample output from the **show ospfv3 virtual-links** command:

```
Router# show ospfv3 virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

The table below describes the significant fields shown in the display.

Table 197: show ospfv3 virtual-links Field Descriptions

Field	Description
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	Specifies the OSPFv3 neighbor, and if the link to that neighbor is up or down.
Interface ID	Interface ID and IPv6 address of the router.
Transit area 2	The transit area through which the virtual link is formed.
via interface ATM3/0	The interface through which the virtual link is formed.
Cost of using 1	The cost of reaching the OSPFv3 neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPFv3 neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:06	When the next hello is expected from the neighbor.

The following sample output from the **show ospfv3 virtual-links** command has two virtual links. One is protected by authentication, and the other is protected by encryption. <<This is show ipv6 ospf virtual-links output--should it be modified/replaced?>>

```
Router# show ospfv3 virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
   Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial12/0, Cost of using 64
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/2/4, retransmission queue length 0, number of retransmission 1
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
   Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial11/0, Cost of using 128
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show platform 6rd tunnel-endpt

To display IPv6 rapid deployment (6RD) information about a tunnel end point, use the **show platform 6rd tunnel-endpt** command in the Privileged EXEC mode.

show platform 6rd tunnel-endpt

Syntax Description

tunnel-endpt	Displays 6rd tunnel end points.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
15.3(2)S	This command was introduced on the Cisco 7600 series routers.

Example

This example displays the total number of tunnel end points configured.

```
Device#show platform 6rd tunnel-endpt
6rd End-pt in use: 1
6rd End-pt in use: 2
6rd End-pt in use: 3
6rd End-pt in use: 4
6rd End-pt in use: 5
6rd End-pt in use: 6
6rd End-pt in use: 7
6rd End-pt in use: 8
6rd End-pt in use: 9
--More--
6rd End-pt in use: 108
6rd End-pt in use: 109
6rd End-pt in use: 110
Total 6rd End-pt in use: 110
```

Related Commands

Command	Description
show tunnel 6rd destination	Translates a 6RD prefix to the corresponding IPv4 destination.
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show platform software ipv6-multicast

To display information about the platform software for IPv6 multicast, use the **show platform software ipv6-multicast**command in privileged EXEC mode.

show platform software ipv6-multicast {**acl-exception** | **acl-table** | **capability** | **connected** | **shared-adjacencies** | **statistics** | **summary**}

Syntax Description

acl-exception	Displays the IPv6-multicast entries that were switched in the software due to ACL exceptions.
acl-table	Displays the IPv6-multicast access list (ACL) request table entries.
capability	Displays the hardware capabilities.
connected	Displays the IPv6-multicast subnet/connected hardware entries.
shared-adjacencies	Displays the IPv6-multicast shared adjacencies.
statistics	Displays the internal software-based statistics.
summary	Displays the IPv6-multicast hardware-shortcut count.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(18)SXE	This command was changed as follows: • Add the **acl-exception**, **acl-table**, and the **statistics**keywords on the Supervisor Engine 720 only. • Update the **show platform software ipv6-multicast capability** command output to include replication information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the IPv6-hardware capabilities:

```
Router# show platform software ipv6-multicast capability
 Hardware switching for ipv6 is Enabled
 (S,G) forwarding for ipv6 supported using Netflow
 (*,G) bridging for ipv6 is supported using Fib
 Directly-connected entries for IPv6 is supported using ACL-TCAM.
Current System HW Replication Mode : Egress
Audo-detection of Replication Mode : ON
Slot Replication-Capability Replication-Mode
```

```
   2 Egress                 Egress
   5 Egress                 Egress
```

This example shows how to display the IPv6-multicast subnet/connected-hardware entries:

```
Router# show platform software ipv6-multicast connected
IPv6 Multicast Subnet entries
Flags : H - Installed in ACL-TCAM
        X - Not installed in ACL-TCAM due to
            label-full exception
Interface: Vlan40 [ H ]
         S:40::1 G:FF00::
         S:0:5000::2 G:FF00::
         S:5000::2 G:FF00::
Interface: Vlan30 [ H ]
         S:30::1 G:FF00::
Interface: Vlan20 [ H ]
         S:20::1 G:FF00::
Interface: Vlan10 [ H ]
         S:10::1 G:FF00::
```

This example shows how to display the IPv6-multicast shared adjacencies:

```
Router# show platform software ipv6-multicast shared-adjacencies

---- SLOT [7] ----
Shared IPv6 Mcast Adjacencies Index  Packets       Bytes
----------------------------- ------ ------------- ------------------
Subnet bridge adjacency       0x7F802  0             0
Control bridge adjacency      0x7      0             0
StarG_M bridge adjacency      0x8      0             0
S_G bridge adjacency          0x9      0             0
Default drop adjacency        0xA      0             0
StarG (spt == INF) adjacency  0xB      0             0
StarG (spt != INF) adjacency  0xC      0             0
```

This example shows how to display the IPv6-multicast statistics information:

```
Router# show platform software ipv6-multicast statistics
IPv6 Multicast HW-switching Status                : Enabled
IPv6 Multicast (*,G) HW-switching Status          : Disabled
IPv6 Multicast Subnet-entries Status              : Enabled
Default MFIB IPv6-table                           : 0x5108F770
(S,G,C) flowmask index                            : 3
(*,G,C) flowmask index                            : 65535
General Counters
--------------------------------------------------+------+
Mfib-hw-entries count                             0
Mfib-add count                                    4
Mfib-modify count                                 2
Mfib-delete count                                 2
Mfib-NP-entries count                             0
Mfib-D-entries count                              0
Mfib-IC-entries count                             0
Error Counters
--------------------------------------------------+------+
ACL flowmask err count                            0
ACL TCAM exptn count                              0
ACL renable count                                 0
Idb Null error                                    0
```

This example shows how to display the IPv6-multicast hardware shortcut count:

```
Router# show platform software ipv6-multicast summary
IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type               Shortcut count
---------------------------+--------------
(S, G)                      0
IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type               Shortcut count
---------------------------+--------------
(*, G/128)                  0
(*, G/m)                    0
```

Related Commands

Command	Description
ipv6 mfib hardware-switching	Configures hardware switching for IPv6 multicast packets on a global basis.

show platform software vpn

To display information about the platform software for IPv6 Virtual Private Networks (VPNs), use the **show platform software vpn** command in privileged EXEC mode.

show platform software vpn [{**status** | **mapping ios**}]

Syntax Description

status	(Optional) Displays the VPN status.
mapping ios	(Optional) Displays the Cisco IOS mapping information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced on the Cisco 7600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If no keyword is used, then all VPN information is displayed.

Examples

The following example shows output regarding platform software for all VPNs:

```
Router# show platform software vpn
```

show tunnel 6rd

To display IPv6 rapid deployment (6RD) information about a tunnel, use the **show tunnel 6rd** command in privileged EXEC mode.

show tunnel 6rd [*tunnel-interface interface-number*]

Syntax Description

tunnel-interface(interface-number	(Optional) Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **show tunnel 6rd** command displays 6RD-related information on a tunnel. If an interface is not specified, information about all the 6RD tunnels on the router is displayed.

Examples

The following is sample output from the show tunnel 6rd command:

```
Router# show tunnel 6rd tunnel 1
show tunnel 6rd tunnel 1
Interface Tunnel1:
  Tunnel Source: 10.1.2.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Prefix, Length: 16, Value: 10.1.0.0
       V4 Suffix, Length: 8, Value: 0.0.0.1
  General Prefix: 2001:B000:200::/40
```

The table below describes the significant fields shown in the display.

Table 198: show tunnel 6rd Field Descriptions

Field	Description
Interface Tunnel1:	The specified tunnel interface and number.
Tunnel Source: 10.1.2.1	The source address for the tunnel interface.
6RD: Operational	6RD is enabled on the router.
V6 Prefix: 2001:B000::/32	The common IPv6 prefix on IPv6 6RD tunnels.
V4 Common Prefix Length: 16, Value: 10.1.0.0	The prefix length and value of the IPv4 transport address common to all the 6RD routers in a domain.
V4 Common Suffix Length: 8, Value: 0.0.0.1	The suffix length and value of the IPv4 transport address common to all the 6RD routers in a domain.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show tunnel 6rd destination

To translate an IPv6 rapid deployment (6RD) prefix to the corresponding IPv4 destination, use the **show tunnel 6rd destination**command in privileged EXEC mode.

show tunnel 6rd destination *ipv6-prefix tunnel-interface interface-number*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix.
tunnel-interface interface-number	Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **show tunnel 6rd destination** command is used to translate a 6RD prefix to the corresponding IPv4 destination. The IPv4 destination address is displayed in the command output.

Examples

The following is sample output from the **show tunnel 6rd destination** command:

```
Router# show tunnel 6rd destination 2001:B000:300:: tunnel 1

Interface: Tunnel1
6RD Prefix: 2001:B000:300::
Destination: 10.1.3.1.
```

Table 199: show tunnel 6rd destination Field Descriptions

Field	Description
Interface Tunnel1:	The specified tunnel interface and number.
6RD Prefix	The specified 6RD IPv6 prefix.
Destination: 10.1.3.1	The corresponding IPv4 destination.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

show tunnel 6rd prefix

To translate an IPv4 destination address to the corresponding IPv6 6RD prefix, use the **show tunnel 6rd prefix** command in privileged EXEC mode.

show tunnel 6rd prefix *ipv4-destination tunnel-interface interface-number*

Syntax Description

ipv4-destination	The IPv4 destination address.
tunnel-interface interface-number	Specifies a tunnel interface and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show tunnel 6rd prefix** command translates an IPv4 destination address to the corresponding IPv6 6RD prefix. The command output displays the 6rd prefix.

Examples

The following is sample output from the **show tunnel 6rd prefix** command:

```
Router# show tunnel 6rd prefix 10.1.3.1 tunnel 0

Interface: Tunnel0
Destination: 10.1.3.1
6RD Prefix: 2001:B000:300::
```

The table below describes the significant fields shown in the display.

Table 200: show tunnel 6rd prefix Field Descriptions

Field	Description
Interface Tunnel0:	The specified tunnel interface and number.
Destination: 10.1.3.1	The IPv4 destination address.
6RD Prefix: 2001:B000:300::	The corresponding 6RD prefix.

Related Commands

Command	Description
tunnel 6rd prefix	Specifies the common IPv6 prefix on IPv6 6RD tunnels.
tunnel mode ipv6ip	Configures a static IPv6 tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

sip address

To configure a Session Initiation Protocol (SIP) server IPv6 address to be returned in the SIP server's IPv6 address list option to clients, use the **sip address**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip address *ipv6-address*
no sip address *ipv6-address*

Syntax Description

ipv6-address	An IPv6 address. The *ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No default behavior or values

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip address** command configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients. To configure multiple SIP server addresses, issue this command multiple times. The new addresses will not overwrite old ones.

Examples

In the following example, the SIP server IPv6 address 2001:0db8::2 is configured to be returned in the SIP server's IPv6 address list option to clients:

```
sip address 2001:0DB8::2
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

sip domain-name

To configure a Session Initiation Protocol (SIP) server domain name to be returned in the SIP server's domain name list option to clients, use the **sip domain-name**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

sip domain-name *domain-name*
no sip domain-name *domain-name*

Syntax Description

domain-name	A domain name for a DHCP for IPv6 client.

Command Default

No default behavior or values.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, the user must also configure the authorization, authentication, and accounting (AAA) client and PPP on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

The **sip domain-name** command configures a SIP server domain name to be returned in the SIP server's domain name list option to clients. To configure multiple SIP server domain names, issue this command multiple times. The new domain names will not overwrite old ones.

Examples

The following example configures the SIP server domain name sip1.cisco.com to be returned in the SIP server's domain name list option to clients:

```
sip domain-name sip1.cisco.com
```

Related Commands

Command	Description
prefix-delegation aaa	Specifies that prefixes are to be acquired from AAA servers.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.

IPv6 Commands: sn to v

sntp address

To specify the IPv6 Simple Network Time Protocol (SNTP) server address list to be sent to the client, use the **sntp address** command in DHCP for IPv6 pool configuration mode. To remove the SNTP server address list, use the **no** form of the command.

sntp address *ipv6-address*
no sntp address *ipv6-address*

Syntax Description

ipv6-address	The IPv6 SNTP address of a server to be sent to the client.

Command Default

No SNTP server address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server address list option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The option defined in this document can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the SNTP server address:

```
sntp address 300::1
```

Related Commands

Command	Description
import sntp address	Imports the SNTP server option to a DHCP for IPv6 client.

spd extended-headroom

To configure Selective Packet Discard (SPD) extended headroom, use the **spd extended-headroom**command in global configuration mode. To return to the default value, use the **no** form of this command.

spd extended-headroom *size*
no spd extended-headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD extended headroom default is 10 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Because Interior Gateway Protocols (IGPs) and link stability are tenuous and crucial, such packets are given the highest priority and are given extended SPD headroom with a default of 10 packets. These packets are not dropped if the size of the input hold queue is lower than 185 (input queue default size + SPD headroom size + SPD extended headroom).

Examples

The following example shows how to configure SPD extended headroom to be 11 packets:

```
Router(config)# spd extended-headroom 11
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd headroom	Configures SPD headroom.

spd headroom

To configure Selective Packet Discard (SPD) headroom, use the **spd headroom**command in global configuration mode. To return to the default value, use the **no** form of this command.

spd headroom *size*
no spd headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD headroom default is 100 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

SPD prioritizes IPv6 packets with a precedence of 7 by allowing the software to queue them into the process level input queue above the normal input queue limit. The number of packets allowed in excess of the normal limit is called the SPD headroom, the default being 100, which means that a high precedence packet is not dropped if the size of the input hold queue is lower than 175 (input queue default size + SPD headroom size).

Examples

The following example shows how to configure SPD headroom to be 95 packets:

```
Router(config)# spd headroom 95
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd extended-headroom	Configures SPD extended headroom.

spf-interval (IPv6)

To configure how often Cisco IOS software performs the shortest path first (SPF) calculation, use the **s pf-interval**command in address family configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval [{**level-1** | **level-2**}] *seconds* [*initial-wait*] [*secondary-wait*]
no spf-interval *seconds*

Syntax Description

level-1	(Optional) Summarizes only routes redistributed into Level 1 with the configured prefix value.
level-2	(Optional) Summarizes routes learned by Level 1 routing into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS also are summarized.
seconds	Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first SPF calculation in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second SPF calculation, in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval**(IPv6) command controls how often Cisco IOS software can perform the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often the SPF calculation is performed, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but it could slow down the rate of convergence.

If IPv6 and IPv4 are configured on the same interface, they must be running the same Intermediate System-to-Intermediate System (IS-IS) level.

You can use the **spf-interval**(IPv6) command only when using the IS-IS multitopology support for IPv6 feature.

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# spf-interval 30
```

Related Commands

Command	Description
prc-interval (IPv6)	Controls the hold-down period between PRCs.

split-horizon (IPv6 RIP)

To configure split horizon processing of IPv6 Routing Information Protocol (RIP) router updates, use the **split-horizon**command in router configuration mode. To disable the split horizon processing of IPv6 RIP updates, use the **no** form of this command.

split-horizon
no split-horizon

Syntax Description

This command has no arguments or keywords.

Command Default

Split horizon is configured and active by default. However, for ATM interfaces and subinterfaces **split-horizon** is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **split-horizon**(IPv6 RIP) command is similar to the **ip split-horizon**command, except that it is IPv6-specific.

This command configures split horizon processing of IPv6 RIP router updates. When split horizon is configured, the advertisement of networks out the interfaces from which the networks are learned is suppressed.

If both split horizon and poison reverse are configured, then split horizon behavior is replaced by poison reverse behavior (routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric).

Note In general, changing the state of the default for the **split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example configures split horizon processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines a neighboring router with which to exchange routing information.

standby ipv6

To ac tivate the Hot Standby Router Protocol (HSRP) in IPv6, use the **standby ipv6** command in interface configuration mode. To disable HSRP, use the **no**form of this command.

standby [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address /prefix-length* | *ipv6-prefix /prefix-lengthlink-local-address* | **autoconfig**}
no standby [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address /prefix-length* | *ipv6-prefix /prefix-lengthlink-local-address* | **autoconfig**}

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
ipv6-global-address	IPv6 address of the hot standby router interface.
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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
link-local-address	Link-local address of the hot standby router interface.
autoconfig	Indicates that a virtual link-local address will be generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

Command Default

The default group number is 0. HSRP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI4	Users can configure a fully routable global virtual IPv6 address.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

An Ethernet or FDDI type interface must be used for HSRP for IPv6. HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

The **standby ipv6** command enables an HSRP group for IPv6 operation. If the **autoconfig** keyword is used, then a link-local address will be generated from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

If an IPv6 global address is used, it must include an IPv6 prefix length. If a link-local address is used, it does not have a prefix.

Examples

The following example enables an HSRP group for IPv6 operation:

```
Router(config)# standby version 2
Router(config)# interface ethernet 0
Router(config-if)# standby ipv6 autoconfig
```

The following example shows three HSRP global IPv6 addresses with an explicitly configured link-local address:

```
interface Ethernet0/0
 no ip address
 ipv6 address 2001::0DB8:1/64
 standby version 2
 standby 1 ipv6 FE80::1:CAFÉ
 standby 1 ipv6 2001::0DB8:2/64
 standby 1 ipv6 2001:0DB8::3/64
 standby 1 ipv6 2001:0DB8::4/64
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

summary-prefix (IPv6 IS-IS)

To create aggregate IPv6 prefixes for Intermediate System-to-Intermediate System (IS-IS), use the **summary-prefix** command in address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *ipv6-prefix/prefix-length*
[{**level-1** | **level-1-2** | **level-2**}] [
tag *tag-value*]
no **summary-prefix** *ipv6-prefix/prefix-length*
[{**level-1** | **level-1-2** | **level-2**}] [
tag]

Syntax Description

ipv6-prefix	Summary prefix designated for a range of IPv6 prefixes. The *ipv6-prefix* 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 comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
level-1	(Optional) Specifies that only routes redistributed into Level 1 are summarized with the configured prefix value.
level-1-2	(Optional) Specifies that summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertises Level 1 routes reachable in its area.
level-2	(Optional) Specifies that routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS will be summarized also.
tag *tag-value*	(Optional) Assigns a tag to an IPV6 summary prefix. The tag value, in the range from 1 to 4294967295, is configured by the **isis ipv6 tag** command.

Command Default

All redistributed routes are advertised individually.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
Cisco IOS XE Release 3.6S	This command was modified. Support for the **tag** keyword was added.

Usage Guidelines

Multiple groups of prefixes can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing updates generated by the router, resulting in shorter routing tables on neighbor routers.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps ensure stability because a summary advertisement is depending on many more specific routes. If one more specific route flaps, in most cases this flapping does not cause a flap of the summary advertisement.

The drawback of summary prefixes is that other routes might have less information with which to calculate the most optimal routing table for all individual destinations.

Note When IS-IS advertises a summary prefix, it automatically inserts the summary prefix into the IPv6 routing table but labels it as a "discard" route entry. Any packet that matches the entry will be discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Examples

In the following example, Routing Information Protocol (RIP) routes are redistributed into IS-IS. The RIP routing table, has IPv6 routes for 3FFE:F000:0001:0000::/64, 3FFE:F000:0002:0000::/64, 3FFE:F000:0003:0000::/64, and so on. This example advertises only 3FFE:F000::/24 into IPv6 IS-IS Level 1.

```
Device(config)# router isis area01
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute rip level-1 metric 40
Device(config-router-af)# summary-prefix 3FFE:F000::/24 level-1
```

The following example shows how to assign a tag to a summary prefix:

```
Device(config)# router isis area01
Device(config-router)# address-family ipv6
Device(config-router-af)# summary-prefix 2001:DB::/24 tag 220
```

Related Commands

Command	Description
isis ipv6 tag	Configures an administrative tag value that will be associated with an IPv6 address prefix and applied to an IS-IS LSP.

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style type, length, and value.
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays information about the IS-IS database.

summary-prefix (OSPFv3)

To configure an IPv6 summary prefix in Open Shortest Path First version 3 (OSPFv3), use the **summary-prefix** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [{**not-advertise** | **tag** *tag-value*}] [**nssa-only**]
no summary-prefix *prefix* [{**not-advertise** | **tag** *tag-value*}] [**nssa-only**]

Syntax Description

prefix	IPv6 route prefix for the destination.
not-advertise	(Optional) Suppresses routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only.
tag *tag-value*	(Optional) Specifies the tag value that can be used as a match value for controlling redistribution via route maps. This keyword applies to OSPFv3 only.
nssa-only	(Optional) Limits the scope of the prefix to the area. Sets the nssa-only attribute for the summary route (if any) generated for the specified prefix.

Command Default

No IPv6 summary prefix is defined.

Command Modes

OSPFv3 router configuration mode (config-router)

IPv6 address family configuration (config-router-af)

IPv4 address family configuration (config-router-af)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(4)S	This command was modified. The **nssa-only** keyword was added.

Release	Modification
15.1(1)SY	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The summary-prefix command can be used to summarize devices redistributed from other routing protocols. Multiple groups of addresses can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Specify the **nssa-only** keyword to clear the propagate bit (P-bit) when external routes are redistributed into a not-so-stubby area (NSSA). Doing so prevents corresponding NSSA external link state advertisements (LSAs) from being translated into other areas.

Examples

In the following example, the summary prefix 2051:0:0:10::/60 includes addresses beginning at 2051:0:0:10::/60 up to (but not including) 2051:0:0:20::/128. Only the address 2051:0:0:10::/60 is advertised in an external LSA:

```
summary-prefix 2051:0:0:10::/60
```

Related Commands

router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

synchronization (IPv6)

To enable the synchronization between IPv6 Border Gateway Protocol (BGP) and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for IGP, use the **no** form of this command.

synchronization
no synchronization

Syntax Description

This command has no arguments or keywords.

Command Default

BGP advertises network routes without waiting for IGP.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Unlike the IPv4 version of the **synchronization** command, the IPv6 version is disabled by default.

By default, an IPv6 BGP speaker advertises an IPv6 network route without waiting for the IGP. Use the **synchronization** command in address family configuration mode to synchronize routing advertisements between BGP and your IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. When synchronization is enabled, IPv6 BGP does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following example enables a router to advertise an IPv6 network route without waiting for an IGP:

```
router bgp 65000
address-family ipv6
 synchronization
```

timers (IPv6 RIP)

To configure update, timeout, hold-down, and garbage-collection timers for an IPv6 RIP routing process, use the **timers**command in router configuration mode. To return the timers to their default values, use the **no** form of this command.

timers *update timeout holddown garbage-collection*
no timers

Syntax Description

update	Interval of time (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.
timeout	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update*argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters a hold-down state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. A route enters a hold-down state when it becomes unreachable and the hold-down timer is a value other than zero. (A learned RIP route becomes unreachable when the route is not refreshed or the route is advertised with a metric of 16.) While in hold-down state, the system ignores any new information about the route from RIP or from any protocols that have a worse administrative distance than RIP. A route with a better administrative distance will replace the unreachable route, even if the route is still in a hold-down state.
garbage-collection	Amount of time (in seconds) that must pass from when a route becomes invalid until the route is removed from the routing table.

Command Default

Update timer: 30 seconds Timeout timer: 180 seconds Hold-down timer: 0 seconds Garbage-collection timer: 120 seconds

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and the hold-down timer default value was changed to 0 seconds.
12.2(13)T	The hold-down timer default value was changed to 0 seconds.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **timers**(IPv6 RIP)command is similar to the **timers basic**(RIP)command, except that it is IPv6-specific.

Use the *update* argument to set the time interval between RIP routing updates. If no route update is received for the time interval specified by the *timeout* argument, the route is considered unreachable. Use the *holddown* argument to set a time delay between the route becoming unreachable and the route being considered invalid in the routing table. The use of a hold-down interval is not recommended for RIP because it can introduce long delays in convergence. Use the *garbage-collection* argument to specify the time interval between a route being considered invalid and the route being purged from the routing table.

The basic timing parameters for IPv6 RIP are adjustable. Because IPv6 RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers and access servers in the network.

Note The current and default timer values are displayed in the output of the **show ipv6 rip** EXEC command. The relationships of the various timers should be preserved, as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a route is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 10 seconds. Assuming no updates, the route is flushed from the routing table 20 seconds after the end of the hold-down period.

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# timers 5 15 10 30
```

Caution By setting a short update period, you run the risk of congesting slow-speed serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the **timers lsa arrival**command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*
no timers lsa arrival

Syntax Description

milliseconds	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.

Command Default

1000 milliseconds

Command Modes

OSPF for IPv6 router configuration (config-rtr) Router configuration (config-router)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We suggest you keep the *milliseconds*value of the **timers lsa arrival** command less than or equal to the neighbors’ *hold-interval* value of the **timers throttle lsa all** command.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
router ospf 1
 log-adjacency-changes
```

```
timers throttle lsa all 200 10000 45000
timers lsa arrival 2000
network 10.10.4.0 0.0.0.255 area 24
network 10.10.24.0 0.0.0.255 area 24
```

Related Commands

Command	Description
show ip ospf timers rate-limit	Displays all of the LSAs in the rate limit queue.
show ipv6 ospf timers rate-limit	Displays all of the LSAs in the IPv6 rate limit queue
timers throttle lsa	Sets rate-limiting values for OSPF for IPv6 LSA generation.
timers throttle lsa all	Sets rate-limiting values for LSAs being generated.

timers pacing flood (OSPFv3)

To configure link-state advertisement (LSA) flood packet pacing, use the **timers pacing flood** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*
no timers pacing flood

Syntax Description

milliseconds	Time (in milliseconds) at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 milliseconds to 100 milliseconds. The default value is 33 milliseconds.

Command Default

The default is 33 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

Configuring Open Shortest Path First version 3 (OSPF) flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 transmission queue. This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs.

The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default flood timer values.

Examples

The following example configures LSA flood packet-pacing updates to occur in 20-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing flood 20
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing lsa-group (OSPFv3)

To change the interval at which Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers pacing lsa-group** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*
no timers pacing lsa-group

Syntax Description

seconds	Number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.

Command Default

The default interval for this command is 240 seconds. OSPFv3 LSA group pacing is enabled by default.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY

Usage Guidelines

This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes the risks associated with changing the default timer values.

Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Examples

The following example configures OSPFv3 group packet-pacing updates between LSA groups to occur in 300-second intervals for OSPFv3 routing process 1:

```
Router(config)#
 router ospfv3 1
Router(config-router)#
 timers pacing lsa-group 300
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission (OSPFv3)

To configure link-state advertisement (LSA) retransmission packet pacing in IPv4 Open Shortest Path First version 3 (OSPFv3), use the **timers pacing retransmission** command in OSPFv3 router configuration mode. To restore the default retransmission packet pacing value, use the **no** form of this command.

timers pacing retransmission *milliseconds*
no timers pacing retransmission

Syntax Description

milliseconds	The time (in milliseconds) at which LSAs in the retransmission queue are paced. The configurable range is from 5 milliseconds to 200 milliseconds. The default value is 66 milliseconds.

Command Default

The default is 66 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Configuring OSPFv3 retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 retransmission queue. This command allows you to control the rate at which LSA updates occur to reduce high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet retransmission pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet retransmission pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 100-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing retransmission 100
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.

timers spf (IPv6)

To turn on Open Shortest Path First (OSPF) for IPv6 shortest path first (SPF) throttling, use the **timers spf** command in router configuration mode. To turn off SPF throttling, use the **no** form of this command.

timers spf *delay holdtime*
no timers spf

Syntax Description

delay	Delay (in milliseconds) in receiving a change in the SPF calculation. The range is from 0 through 4294967295. The default is 5 milliseconds.
holdtime	Hold time (in milliseconds) between consecutive SPF calculations. The range is from 0 through 4294967295. The default is 10 milliseconds.

Command Default

OSPF for IPv6 throttling is always enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *delay* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *holdtime* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Examples

The following example shows a router configured with the delay and hold-time interval values for the **timers spf** command set at 40 and 50 milliseconds, respectively.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# timers spf 40 50
```

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.

timers throttle lsa

To set rate-limiting values for Open Shortest Path First (OSPF) for IPv6 link-state advertisement (LSA) generation, use the **timers throttle lsa**command in router configuration mode. To restore the default values, use the **no** form of this command.

timers throttle lsa *start-interval hold-interval max-interval*
no timers throttle lsa

Syntax Description

start-interval	Minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF for IPv6 topology change. The generation of the next LSA is not before the start interval. The range is from 0 to 600,000 milliseconds. The default is 0 milliseconds, which means no delay; the LSA is sent immediately.
hold-interval	Incremental time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Maximum wait time in milliseconds between generation of the same LSA. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.

Command Default

start-interval : 0 milliseconds*hold-interval:*5000 milliseconds*max-interval*: 5000 milliseconds

Command Modes

OSPF for IPv6 router configuration (config-rtr)
Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. We suggest you keep the *milliseconds*value of the **timers lsa arrival**command less than or equal to the *hold-interval* value of the **timers throttle lsa**command.

Examples

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

This example customizes IPv6 OSPF LSA throttling so that the start interval is 500 milliseconds, the hold interval is 1,000 milliseconds, and the maximum interval is 10,000 milliseconds.

```
ipv6 router ospf 1
 log-adjacency-changes
 timers throttle lsa 500 1000 10000
```

Related Commands

Command	Description
show ipv6 ospf	Displays information about OSPF for IPv6 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

timers throttle spf

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*
no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial delay to schedule an SPF calculation after a change, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 5000.
spf-hold	Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.
spf-max-wait	Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.

Command Default

SPF throttling is not set.

Command Modes

Address family configuration (config-router-af) Router address family topology configuration (config-router-af-topology) Router configuration (config-router) OSPF for IPv6 router configuration (config-rtr)

Command History

Release	Modification
12.2(14)S	This command was introduced. This command replaces the **timers spf-interval** command.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added and this command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start*argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-max-wait* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **timers throttle spf** command in router address family topology configuration mode in order to make this OSPF router configuration command become topology-aware.

Release 15.2(1)T

When you configure the **ospfv3 network manet** command on any interface attached to the OSPFv3 process, the default values for the *spf-start*, *spf-hold*, and the *spf-max-wait* arguments are reduced to 1000 milliseconds, 1000 milliseconds, and 2000 milliseconds respectively.

Examples

The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds, respectively.

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 10.21.21.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 00
```

The following example shows how to configure a router using IPv6 with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 500, 1000, and 10,000 milliseconds, respectively.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
 log-adjacency-changes
 timers throttle spf 500 1000 10000
```

Related Commands

Command	Description
ospfv3 network manet	Sets the network type to Mobile Ad Hoc Network (MANET).

tracking

To override the default tracking policy on a port, use the **tracking**command in Neighbor Discovery (ND) inspection policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

Syntax Description

enable	Tracking is enabled.
reachable-lifetime	(Optional) The maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

ND inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through ND inspection. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **stale-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.
ipv6 neighbor tracking	Enables tracking of entries in the binding table.

trusted

To allow hardware bridging for all data traffic on the target where the policy is applied, use the **trusted** command in source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode. To disallow hardware bridging, use the **no** form of this command.

trusted
no trusted

Syntax Description

This command has no arguments or keywords.

Command Default

Hardware bridging is not allowed on the target on which the policy is applied.

Command Modes

Source-guard policy configuration mode (config-source-guard)

Command History

Release	Modification
15.3(1)S	This command was introduced.

Usage Guidelines

Use the **trusted** command to allow hardware bridging for all data traffic on the target where the source-guard policy is applied. This function disables a source-guard policy on specific ports when IPv6 source guard is configured on a VLAN target.

Examples

```
Device(config)# ipv6 source-guard policy
Device(config-source-guard)# deny global-autoconf
Device(config-source-guard)# trusted
```

Related Commands

Command	Description
deny global-autoconfig	Denies data traffic from autoconfigured global addresses.
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

trusted-port (IPv6 NDP Inspection Policy)

To configure a port to become a trusted port, use the **trusted-port** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode . To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

NDP inspection policy configuration
(config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Use the **trusted-port** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.

trusted-port (IPv6 RA Guard Policy)

To configure a port to become a trusted port, use the **trusted-port**command in router advertisement (RA) guard policy configuration . To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, the **device-role** command takes precedence over the **trusted-port** command; if the device role is configured as host, messages will be dropped regardless of **trusted-port** command configuration.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-ra-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

tunnel 6rd br

To bypass security checks on an IPv6 rapid deployment (6RD) customer-edge (CE) router, use the **tunnel 6rd br command** in interface configuration mode. To remove the BR router's address from configuration, use the **no** form of this command.

tunnel 6rd br *ipv4-address*
no tunnel 6rd br *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the BR router.

Command Default

No BR router is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd br** command is optional for 6RD operation. The command allows the user to specify the BR address, which allows the 6RD router to skip the security checks for packets from that source.

By default at a 6RD router, all incoming packets require that their outer IPv4 source address to be embedded in the 6RD-encoded IPv6 source address. Packets that do not satisfy this criteria are dropped. Configuring the **tunnel 6rd br** command exempts packets with the specified source from this check.

The **tunnel 6rd br** command should be enabled on the customer edge (CE) router, because packets arriving at the CE from the BR typically are traffic from a native IPv6 host, which does not need to have a 6RD-encoded source address.

Examples

The following example sets the BR address to 10.1.4.1:

```
Router(config-if)# tunnel 6rd br 10.1.4.1
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd ipv4

To specify the prefix length and suffix length of the IPv4 transport address common to all the 6RD routers in a domain, use the tunnel 6rd ipv4 command in interface configuration mode. To remove these parameters, use the **no** form of this command.

tunnel 6rd ipv4 prefix-len *length* **suffix-len** *length*
no tunnel 6rd ipv4 prefix-len *length* **suffix-len** *length*

Syntax Description

prefix-len *length*	Specifies the prefix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.
suffix-len *length*	Specifies the suffix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.

Command Default

The prefix length and suffix length are 0.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd ipv4**command is optional for 6RD operation. This command specifies the number of most significant bits and least significant bits of the IPv4 transport address (that is, the tunnel source) that are common to all the 6RD routers in a domain. The valid range is from 0 to 31, and the sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31. If the **tunnel 6rd ipv4**command is not configured, and the **tunnel 6rd prefix** command is configured, the system uses the default value of 0.

Examples

The following example shows 6RD configuration, including the number of most and least significant bits of the IPv4 transport address common to all the 6RD routers in a domain:

```
Router(config)# interface Tunnel1
Router(config-if)# ipv6 address 2001:B000:100::1/32
Router(config-if)# tunnel source GigabitEthernet2/0/0
Router(config-if)# tunnel mode ipv6ip 6rd
Router(config-if)# tunnel 6rd prefix 2001:B000::/32
Router(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel 6rd prefix	Specifies the common IPv6 prefix on 6RD tunnels
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd prefix

To specify the common IPv6 prefix on IPv6 rapid deployment (6RD) tunnels, use the tunnel 6rd prefix command in interface configuration mode. To remove the IPv6 prefix, use the **no** form of this command.

tunnel 6rd prefix *ipv6-prefix /prefix-length*
no tunnel 6rd prefix *ipv6-prefix /prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

This command can be enabled only when 6RD is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd prefix** command is mandatory for 6RD operation. It specifies the common IPv6 prefix, and the *prefix-length* argument determines us the position of the IPv4 address in the 6RD delegated prefix (or payload) destination. Configuring a *prefix-length* of 0 is equivalent to removing this command.

The tunnel line state of a 6RD tunnel remains inactive until the **tunnel 6rd prefix**command is configured, and this command is automatically disabled when the **tunnel mode ipv6ip**command is configured to use a keyword other than **6rd**.

Examples

The following example shows 6RD configuration, including the **tunnel 6rd prefix** command:

```
ipv6 general-prefix 6rd1 6rd Tunnel1
!
interface Tunnel1
 ipv6 address 6rd1 ::1/124
tunnel source GigabitEthernet2/0/0
tunnel mode ipv6ip 6rd
tunnel 6rd prefix 2001:B000::/32
tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.

Command	Description
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel mode ipv6ip

To configure a static IPv6 tunnel interface, use the **tunnel mode ipv6ip** command in interface configuration mode. To remove a static IPv6 tunnel interface, use the **no** form of this command.

tunnel mode ipv6ip [{**6rd** | **6to4** | **auto-tunnel** | **isatap**}]
no tunnel mode ipv6ip

Syntax Description

6rd	(Optional) Specifies that the tunnel is to be used for IPv6 rapid deployment (6RD).
6to4	(Optional) Configures an IPv6 automatic tunnel using a destination address that is dynamically constructed from an IPv4 address and the prefix 2002::/16 (referred to as a 6to4 address).
auto-tunnel	(Optional) Configures an IPv6 automatic tunnel using an IPv4-compatible IPv6 address.
isatap	(Optional) Configures an IPv6 automatic tunnel using Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) to connect IPv6 nodes (hosts and routers) within IPv4 networks.

Command Default

Static IPv6 tunnel interfaces are not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was modified. The **isatap** keyword was added to support the addition of ISATAP tunnel implementation.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	This command was modified. The **6rd** keyword was added. The **auto-tunnel** keyword was deprecated on Cisco ASR 1000 series routers.
15.1(3)T	This command was modified. The **6rd** keyword was added.
15.1SY	This command was integrated into Cisco IOS Release 15.1SY. The **auto-tunnel** keyword was deprecated.

Release	Modification
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

IPv6 tunneling is the encapsulation of IPv6 packets within IPv4 packets and transmitting the packets across an IPv4 routing infrastructure.

Manually Configured Tunnels

The **tunnel mode ipv6ip** command configures an IPv6 tunnel. The devices at each end of the IPv6 tunnel must support both IPv4 and IPv6 protocol stacks.

To use this command, you must first manually configure the following:

- An IPv6 address on the tunnel interface
- An IPv4 address as the tunnel source
- An IPv4 address as the tunnel destination

Automatic Determination of Tunnel Destination

The **tunnel mode ipv6ip auto-tunnel** command configures an automatic IPv6 tunnel. The tunnel source is manually configured. The tunnel destination is automatically determined as the low-order 32 bits of the IPv4-compatible IPv6 addresses. An IPv4-compatible IPv6 address is a 128-bit IPv6 address that contains the IPv6 prefix 0:0:0:0:0:0 in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits of the address. The devices at each end of the automatic tunnel must support both IPv4 and IPv6 protocol stacks.

6to4 Tunnels

The **tunnel mode ipv6ip 6to4** command configures an automatic 6to4 tunnel where the tunnel endpoint is determined by a globally unique IPv4 address embedded into a 6to4 address. A 6to4 address is a combination of the prefix 2002::/16 and a globally unique 32-bit IPv4 address. (IPv4-compatible addresses are not used in 6to4 tunneling.) The unique IPv4 address is used as the network-layer address in the 6to4 address prefix. The source of the tunnel is an interface that you can manually configure using the **tunnel source** command. The border devices at each end of a 6to4 tunnel must support both IPv4 and IPv6 protocol stacks. Additionally, the traffic that is destined for the network with the 6to4 address prefix must be routed over the tunnel by using the **ipv6 route** command.

6RD Tunnels

The **tunnel mode ipv6ip 6rd** command specifies that the tunnel is to be used for IPv6 RD. The 6RD feature is similar to the 6to4 tunnel feature, but it does not require addresses to have a 2002::/16 prefix. It also does not require that all 32 bits of the IPv4 destination be in the IPv6 payload header.

ISATAP Tunnels

ISATAP tunnels enable the transportation of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4 or IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

Unlike IPv4-compatible addresses, ISATAP IPv6 addresses can use any initial unicast /64 prefix. The last 64 bits are used as the interface identifier. Of these, the first 32 bits are the fixed pattern 0000:5EFE. The last 32 bits carry the tunnel endpoint IPv4 address.

Examples

Manually Configured IPv6 Tunnel Example

The following example shows how to configure a manual IPv6 tunnel. In this example, tunnel interface 0 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured.

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 192.168.30.1
Device(config-if)# tunnel mode ipv6ip
Device(config-if)# end
```

IPv4 Compatible IPv6 Address Tunnel Example

The following example shows how to configure an automatic IPv6 tunnel that uses Ethernet interface 0 as the tunnel source. The tunnel destination is determined automatically as the low-order 32 bits of an IPv4-compatible IPv6 address.

```
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip auto-tunnel
Device(config-if)# end
```

6to4 Tunnel Example

The following example shows how to configure a 6to4 tunnel. In this example, Ethernet interface 0 is configured with an IPv4 address 192.168.99.1. The site-specific 48-bit prefix 2002:c0a8:630 is constructed by prepending the prefix 2002::/16 to the IPv4 address 192.168.99.1.

The tunnel interface 0 is configured without an IPv4 or IPv6 address. The tunnel source address is configured manually as Ethernet interface 0. The tunnel destination address is automatically constructed. An IPv6 static route is configured to route traffic that is destined for network 2002::/16 over tunnel interface 0.

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 192.168.99.1 255.255.255.0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# exit
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# ipv6 route 2002::/16 tunnel 0
Device(config)# end
```

Tunnel Interface Configured with theipv6 unnumbered Command Example

When a tunnel interface is configured using the **ipv6 unnumbered**, **tunnel source**, and **tunnel mode ipv6ip** commands, the tunnel uses the first IPv6 address configured on the source interface as its IPv6 address. For 6to4 tunnels, the first IPv6 address configured on the source interface must be a 6to4 address. In the following example, the first IPv6 address configured for Ethernet interface 0 (6to4 address 2002:c0a8:6301:1::/64) is used as the IPv6 address of tunnel 0:

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# ipv6 address 3ffe:1234:5678::1/64
Device(config-if)# end
```

6RD Tunnel Example

The following example shows how to configure a 6RD tunnel:

```
Device(config)# interface Tunnel1
Device(config-if)# ipv6 address 2001:B000:100::1/32
Device(config-if)# tunnel source GigabitEthernet2/0/0
Device(config-if)# tunnel mode ipv6ip 6rd
Device(config-if)# tunnel 6rd prefix 2001:B000::/32
Device(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
Device(config-if)# end
Device# show tunnel 6rd Tunnel1

Interface Tunnel1:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Common Prefix Length: 16, Value: 10.1.0.0
       V4 Common Suffix Length: 8, Value: 0.0.0.1
```

ISATAP Tunnel Example

The following example shows how to configure ISATAP tunnel over an Ethernet interface 0. Router advertisements are enabled to allow client autoconfiguration.

```
Device(config)# interface Ethernet 0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip isatap
Device(config-if)# ipv6 address 2001:0DB8::/64 eui-64
Device(config-if)# no ipv6 nd ra suppress
Device(config-if)# end
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
ipv6 address eui-64	Configures an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 route	Establishes static IPv6 routes.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 nd ra suppress	Reenables the sending of IPv6 router advertisement transmissions on a LAN interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show tunnel 6rd tunnel	Displays 6RD information about a tunnel.
tunnel 6rd ipv4	Specifies the prefix length and suffix length of the IPv4 transport address that is common to all the 6RD routers in a domain.
tunnel 6rd prefix	Specifies the common IPv6 prefix on 6RD tunnels.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

validate source-mac

To check the source media access control (MAC) address against the link-layer address, use the **validate source-mac**command in Neighbor Discovery (ND) inspection policy configuration mode .

validate source-mac
no validate source-mac

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

When the router receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. Use the **validate source-mac** command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Examples

The following example enables the router to drop an ND message whose link-layer address does not match the MAC address:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# validate source-mac
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy n ame and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

vrf (DHCPv6 pool)

To associate a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address pool with a virtual private network (VPN) routing and forwarding (VRF) instance, use the **vrf** command in DHCPv6 pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*
no vrf *name*

Syntax Description

name	Name of the VRF with which the address pool is associated.

Command Default

No VRF is associated with the DHCPv6 address pool.

Command Modes

DHCPv6 pool configuration (config-dhcp)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Examples

The following example shows how to configure an IPv6 pool named pool1, and associate pool1 with a VRF instance named vrf1:

```
Router(config)# ipv6 dhcp pool pool1
# vrf vrf1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.