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.