IPv6 Commands: ipv6 h to ipv6 mi

ipv6 hello-interval eigrp

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by an autonomous system number, use the **ipv6 hello-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hello-interval eigrp *as-number seconds*

no ipv6 hello-interval eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hello interval is 60 seconds. For all other networks, the default hello interval is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of EIGRP for IPv6, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds on autonomous system 1:

```
interface ethernet 0
 ipv6 hello-interval eigrp 1 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hold-time eigrp	Configures the hold time for a particular EIGRP for IPv6 routing process designated by the autonomous system number.

ipv6 hold-time eigrp

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing process designated by the autonomous system number, use the **ipv6 hold-time eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 hold-time eigrp *as-number seconds*

no ipv6 hold-time eigrp *as-number seconds*

Syntax Description

as-number	Autonomous system number.
seconds	Hello interval, in seconds. The range is from 1 to 65535.

Command Default

For low-speed, nonbroadcast multiaccess (NBMA) networks, the default hold-time interval is 180 seconds. For all other networks, the default hold-time interval is 15 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

Cisco recommends that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds for AS 1:

```
interface ethernet 0
 ipv6 hold-time eigrp 1 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ipv6 hello-interval eigrp	Configures the hello interval for the EIGRP for IPv6 routing process designated by an autonomous system number.

ipv6 hop-limit

To configure the maximum number of hops used in router advertisements and all IPv6 packets that are originated by the router, use the **ipv6 hop-limit**command in global configuration mode. To return the hop limit to its default value, use the **no** form of this command.

ipv6 hop-limit *value*

no ipv6 hop-limit *value*

Syntax Description

value	The maximum number of hops. The acceptable range is from 1 to 255.

Command Default

The default is 64 hops.

Command Modes

Global configuration

Command History

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

Examples

The following example configures a maximum number of 15 hops for router advertisements and all IPv6 packets that are originated from the router:

```
Router(config)# ipv6 hop-limit 15
```

ipv6 host

To define a static host name-to-address mapping in the host name cache, use the **ipv6 host**command in global configuration mode. To remove the host name-to-address mapping, use the no form of this command.

ipv6 host *name* [*port*] *ipv6-address*

no ipv6 host *name*

Syntax Description

name	Name of the IPv6 host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
port	(Optional) The default Telnet port number for the associated IPv6 addresses.
ipv6-address	Associated IPv6 address. You can bind up to four addresses to a host name.

Command Default

Static host name-to-address mapping in the host name cache is not defined. The default Telnet port is 23.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The first character of the *name* variable can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
Device(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Device(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

Related Commands

Command	Description
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

ipv6 icmp error-interval

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

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

no ipv6 icmp error-interval

Syntax Description

milliseconds	The time interval between tokens being placed in the bucket. The acceptable range is from 0 to 2147483647 with a default of 100 milliseconds.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200 with a default of 10 tokens.

Command Default

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero. The time interval between tokens placed in the bucket is 100 milliseconds. The maximum number of tokens stored in the bucket is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	Support for IPv6 ICMP rate limiting was extended to use token buckets.
12.0(21)ST	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command, with the support for IPv6 ICMP rate limiting extended to use token buckets, was integrated into Cisco IOS Release 12.0(23)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

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 integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

The *milliseconds* argument specifies the time interval between tokens arriving in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

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

Examples

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

```
ipv6 icmp error-interval 50 20
```

Related Commands

Command	Description
show ipv6 traffic	Displays statistics about IPv6 traffic.

ipv6 inspect

To apply a set of inspection rules to an interface, use the **ipv6 inspect** command in interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

ipv6 inspect *inspection-name* {**in**| **out**}

no ipv6 inspect *inspection-name* {**in**| **out**}

Syntax Description

inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

Command Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by Context-Based Access Control (CBAC).

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an inbound packet.

Examples

The following example applies a set of inspection rules named "outboundrules" to an external interface's outbound traffic. This causes inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
 ipv6 inspect outboundrules out
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of inspection rules.

ipv6 inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the ipv6 inspect alert off command in global configuration mode. To enable Cisco IOS firewall alert messages, use the no form of this command.

ipv6 inspect alert-off

no ipv6 inspect alert-off

Syntax Description

This command has no arguments or keywords.

Command Default

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example turns off CBAC alert messages:

```
ipv6 inspect alert-off
```

Related Commands

Command	Description
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each Cisco IOS firewall session closes, use the ipv6 inspect audit trail command in global configuration mode. To turn off Cisco IOS firewall audit trail message, use the no form of this command.

ipv6 inspect audit trail

no ipv6 inspect audit trail

Syntax Description

This command has no arguments or keywords.

Command Default

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ipv6 inspect audit trail
```

Afterward, audit trail messages such as the following are displayed:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes -- responder
 (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder
 (192.168.129.11:21) sent 325 bytes
```

These messages are examples of audit trail messages. To determine which protocol was inspected, refer to the responder's port number. The port number follows the responder's IP address.

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the ipv6 inspect max-incomplete high command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the no form of this command.

ipv6 inspect max-incomplete high *number*

no ipv6 inspect max-incomplete high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions. The value range is 1 through 4294967295.

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ipv6 inspect max-incomplete low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ipv6 inspect max-incomplete low *number*

no ipv6 inspect max-incomplete low

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect name

To define a set of ipv6 inspection rules, use the **ipv6 inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

ipv6 inspect name *inspection-name protocol* [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

no ipv6 inspect name inspection-name [protocol]

Syntax Description

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.
protocol	A specified protocol. Possible protocol values are **icmp**, **udp**, **tcp**, and **ftp**. This value is optional in the **no** version of this command.
alert {**on** | **off**}	(Optional) For each inspected protocol, the generation of alert messages can be set be on or off. If no option is selected, alerts are generated based on the setting of the ipv6 inspect alert-off command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, the audit trail can be set on or off. If no option is selected, audit trail messages are generated based on the setting of the **ipv6 inspect audit-trail** command.
timeout *seconds*	(Optional) Specifies the number of seconds for a different idle timeout to override the global TCP or User Datagram Protocol (UDP) idle timeouts for the specified protocol. This timeout overrides the global TCP and UPD timeouts but will not override the global Domain Name System (DNS) timeout.

timeout seconds (fragmentation)	Configures the number of seconds that a packet state structure remains active. When the **timeout** value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default **timeout** value is 1 second. If this number is set to a value greater than 1 second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

Command Default

No set of inspection rules is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	FTP protocol support was added.

Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character limit. Define either one or two sets of rules per interface--you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or Internet Control Message Protocol (ICMP) as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol. To remove the entire set of named inspection rules, use the **no** form of this command with the specified inspection name.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return

packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (destination unreachable, echo-reply, time-exceeded, and packet too big) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

FTP Inspection

Cisco IOS Firewall uses layer 7 support for application modules such as FTP.

Cisco IOS IPv6 Firewall uses RFC 2428 to garner IPv6 addresses and corresponding ports. If an address other than an IPv6 address is present, the FTP data channel is not opened.

IPv6-specific port-to-application mapping (PAM) provides FTP inspection. PAM translates TCP or UDP port numbers into specific network services or applications. By mapping port numbers to network services or applications, an administrator can force firewall inspection on custom configurations not defined by well-known ports. PAM delivers with the standard well-known ports defined as defaults.

The table below describes the transport-layer and network-layer protocols.

Table 1: Protocol Keywords--Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	**icmp**
TCP	**tcp**
UDP	**udp**
FTP	**ftp**

Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ipv6 inspect name myrules tcp
ipv6 inspect name myrules udp audit-trail on
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ipv6 inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ipv6 inspect one-minute high**command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ipv6 inspect one-minute high *number*

no ipv6 inspect one-minute high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions . The default is 500 half-open sessions. Value range is 1 through 4294967295

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially-decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ipv6 inspect one-minute low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ipv6 inspect one-minute low *number*

no ipv6 inspect one-minute low

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect routing-header

To specify whether Context-based Access Control (CBAC) should inspect packets containing an IPv6 routing header, use the **ipv6 inspect routing-header** command. To drop packets containing an IPv6 routing header, use the no form of this command.

ipv6 inspect routing-header

no ipv6 inspect routing-header

Syntax Description

This command has no arguments or keywords.

Command Default

Packets containing IPv6 routing header are dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An IPv6 source uses the routing header to list one or more intermediate nodes to be visited between the source and destination of the packet. The Cisco IOS firewall uses this header to retrieve the destination host address. Cisco IOS firewall will establish the appropriate inspection session based on the retrieved address from the routing header.

The originating node lists all intermediate nodes that the packet must traverse. The source and destination address pair in the IPv6 header identifies the hop between the originating node and the first intermediate node. Once the first intermediate node receives the packet, it looks for a routing header. If the routing header is present, the next intermediate node address is swapped with the destination address in the IPv6 header and the packet is forwarded to the next intermediate node. This sequence continues for each intermediate node listed in the routing until no more entries exist in the routing header. The last entry in the routing header is the final destination address.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ip inspect routing-header
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.

Command	Description
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect tcp finwait-time

To define how long a TCP session will be managed after the firewall detects a finish (FIN)-exchange, use the **ipv6 inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ipv6 inspect tcp finwait-time *seconds*

no ipv6 inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds. Valid values are from 1 to 2147483. If the FIN-exchange completes within the configured finwait time, the connection is closed normally.

Command Default

The default is 5 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-Based Access Control (CBAC) inspection is configured for the protocol of the packet, the software establishes state information for the new session.

Use this command to define how long a TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close. In a TCP connection, the client and the server terminate their end of the connection by sending a FIN message. The time that the client and the server wait for their FIN message to be acknowledged by each other before closing the sequence during a TCP connection is called the finwait time. The timeout that you set for the finwait time is referred to as the finwait timeout.

The global value specified for the finwait timeout applies to all TCP sessions inspected by CBAC.

Examples

The following example shows how to change the finwait timeout to 10 seconds:

```
ipv6 inspect tcp finwait-time 5
```

The following example shows how to change the finwait timeout back to the default (5 seconds):

```
no ipv6 inspect tcp finwait-time
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of IPv6 inspection rules.

ipv6 inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ipv6 inspect tcp idle-time** command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

ipv6 inspect tcp idle-time *seconds*

no ipv6 inspect tcp idle-time

Syntax Description

seconds	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).

Command Default

The default is 3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ipv6 inspect name** (global configuration) command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ipv6 inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ipv6 inspect tcp idle-time
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of IPv6 inspection rules.

ipv6 inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the **ipv6 inspect tcp max-incomplete host**command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

ipv6 inspect tcp max-incomplete host *number* **block-time** *minutes*

no ipv6 inspect tcp max-incomplete host

Syntax Description

number	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions. Value range is 1 through 4294967295
block-time	Specifies blocking of connection initiation to a host. Value range is 0 through 35791.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.

Command Default

The default is 50 half-open sessions and 0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, "half-open" means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *minutes* timeout is 0 (the default):

The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections inspected by Context-based Access Control (CBAC).

Examples

The following example changes the **max-incomplete host** number to 40 half-open sessions, and changes the **block-time** timeout to 2 minutes (120 seconds):

```
ipv6 inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ipv6 inspect tcp max-incomplete host
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ipv6 inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ipv6 inspect tcp synwait-time**command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ipv6 inspect tcp synwait-time *seconds*

no ipv6 inspect tcp synwait-time

Syntax Description

seconds	Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session . The default is 30 seconds. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the session's first SYN bit is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

Examples

The following example changes the "synwait" timeout to 20 seconds:

```
ipv6 inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ipv6 inspect tcp synwait-time
```

Related Commands

Command	Description
ipv6 inspect udp idle-time	Specifies the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity).

ipv6 inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the **ipv6 inspect udp idle-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ipv6 inspect udp idle-time *seconds*

no ipv6 inspect udp idle-time

Syntax Description

seconds	Specifies the length of time a UDP "session" will still be managed while there is no activity . The default is 30 seconds. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ipv6 inspect name**command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ipv6 inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ipv6 inspect udp idle-time
```

ipv6 local policy route-map

To enable local policy-based routing (PBR) for IPv6 packets, use the **ipv6 local policy route-map** command in global configuration mode. To disable local policy-based routing for IPv6 packets, use the **no** form of this command.

ipv6 local policy route-map *route-map-name*

no ipv6 local policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to be used for local IPv6 PBR. The name must match a *route-map-name* value specified by the **route-map** command.

Command Default

IPv6 packets are not policy routed.

Command Modes

Global configuration (config#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Packets originating from a router are not normally policy routed. However, you can use the **ipv6 local policy route-map** command to policy route such packets. You might enable local PBR if you want packets originated at the router to take a route other than the obvious shortest path.

The **ipv6 local policy route-map** command identifies a route map to be used for local PBR. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which packets should be policy routed. The **set** commands specify set actions, which are particular policy routing actions to be performed if the criteria enforced by the **match** commands are met. The **no ipv6 local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples

In the following example, packets with a destination IPv6 address matching that allowed by access list pbr-src-90 are sent to the router at IPv6 address 2001:DB8::1:

```
ipv6 access-list src-90
 permit ipv6 host 2001::90 2001:1000::/64
route-map pbr-src-90 permit 10
 match ipv6 address src-90
 set ipv6 next-hop 2001:DB8::1
ipv6 local policy route-map pbr-src-90
```

Related Commands

Command	Description
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to be used to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 local pool

To configure a local IPv6 prefix pool, use the ipv6 local pool configuration command with the prefix pool name. To disband the pool, use the **no** form of this command.

ipv6 local pool poolname prefix/prefix-length assigned-length [shared] [**cache-size** *size*]

no ipv6 local pool poolname

Syntax Description

poolname	User-defined name for the local prefix pool.
prefix	IPv6 prefix assigned to the pool. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix assigned to the pool. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
assigned-length	Length of prefix, in bits, assigned to the user from the pool. The value of the *assigned-length* argument cannot be less than the value of the / *prefix-length* argument.
shared	(Optional) Indicates that the pool is a shared pool.
cache-size *size*	(Optional) Specifies the size of the cache.

Command Default

No pool is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

All pool names must be unique.

IPv6 prefix pools have a function similar to IPv4 address pools. Contrary to IPv4, a block of addresses (an address prefix) are assigned and not single addresses.

Prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, the pool must be removed and recreated. All prefixes already allocated will also be freed.

Examples

This example shows the creation of an IPv6 prefix pool:

```
Router (config)# ipv6 local pool pool1 2001:0DB8::/29 64
Router# show ipv6 local pool
Pool Prefix Free In use
pool1  2001:0DB8::/29  65516  20
```

Related Commands

Command	Description
debug ipv6 pool	Enables IPv6 pool debugging.
peer default ipv6 address pool	Specifies the pool from which client prefixes are assigned for PPP links.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 local pool	Displays information about any defined IPv6 address pools.

ipv6 mfib

To reenable IPv6 multicast forwarding on the router, use the **ipv6 mfib** command in global configuration mode. To disable IPv6 multicast forwarding on the router, use the **no** form of this command.

ipv6 mfib

no ipv6 mfib

Syntax Description

The command has no arguments or keywords.

Command Default

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, IPv6 multicast forwarding is enabled. Because IPv6 multicast forwarding is enabled by default, use the **no** form of the **ipv6 mfib**command to disable IPv6 multicast forwarding.

Examples

The following example disables multicast forwarding on the router:

```
no ipv6 mfib
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 mfib-cef

To enable Multicast Forwarding Information Base (MFIB) Cisco Express Forwarding-based (interrupt level) IPv6 multicast forwarding for outgoing packets on a specific interface, use the **ipv6 mfib-cef**command in interface configuration mode. To disable CEF-based IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib-cef

no ipv6 mfib-cef

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Cisco Express Forwarding-based (interrupt level) IPv6 multicast forwarding is enabled by default when you enable Cisco Express Forwarding-based IPv6 multicast routing.

Use the **show ipv6 mfib interface** command to display the multicast forwarding interface status.

Examples

This example shows how to enable Cisco Express Forwarding-based IPv6 multicast forwarding:

```
Router(config-if)# ipv6 mfib-cef
```

This example shows how to disable Cisco Express Forwarding-based IPv6 multicast forwarding:

```
Router(config-if)# no ipv6 mfib-cef
```

Related Commands

Command	Description
show ipv6 mfib interface	Displays information about IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib cef output

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib cef output**command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib cef output

no ipv6 mfib cef output

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib cef output**command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib cef output
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib interface	Displays IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib fast

Note Effective in Cisco IOS Release 12.3(4)T, the **ipv6 mfib fast**command is replaced by the **ipv6 mfib cef output**command. See the **ipv6 mfib cef output**command for more information.

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib fast**command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib fast

no ipv6 mfib fast

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco Express Forwarding-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(4)T	The command was replaced by the ipv6 mfib cef output command.
12.2(25)S	The command was replaced by the ipv6 mfib cef output command.
12.0(28)S	The command was replaced by the ipv6 mfib cef output command.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib fast** command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib fast
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
show ipv6 mfib interface	Displays IPv6 multicast-enabled interfaces and their forwarding status.

ipv6 mfib forwarding

To enable IPv6 multicast forwarding of packets received from a specific interface on the router, use the **ipv6 mfib forwarding**command in interface configuration mode. To disable IPv6 multicast forwarding of packets received from a specific interface, use the **no** form of this command.

ipv6 mfib forwarding

no ipv6 mfib forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **no ipv6 mfib forwarding** command is used to disable multicast forwarding of packets received from a specified interface, although the specified interface on the router will still continue to receive multicast packets destined for applications on the router itself.

Because multicast forwarding is enabled automatically when IPv6 multicast routing is enabled, the **ipv6 mfib forwarding** command is used to reenable multicast forwarding of packets if it has been previously disabled.

Examples

The following example shows how to disable multicast forwarding of packets from Ethernet 1/1:

```
Router(config) interface Ethernet1/1
Router(config-if) no ipv6 mfib forwarding
```

Related Commands

Command	Description
ipv6 mfib	Reenables IPv6 multicast forwarding on the router.

ipv6 mfib hardware-switching

To configure Multicast Forwarding Information Base (MFIB) hardware switching for IPv6 multicast packets on a global basis, use the **ipv6 mfib hardware-switching** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 mfib hardware-switching [**connected**| **issu-support**| **replication-mode ingress**| **shared-tree**| **uplink**]

no ipv6 mfib hardware-switching [**connected**| **issu-support**| **replication-mode ingress**| **shared-tree**| **uplink**]

Syntax Description

connected	(Optional) Allows you to download the interface and mask entry, and installs subnet entries in the access control list (ACL)-ternary content addressable memory (TCAM).
issu-support	(Optional) Enables In-Service Software Upgrade (ISSU) support for IPv6 multicast.
replication-mode ingress	(Optional) Sets the hardware replication mode to ingress.
shared-tree	(Optional) Sets the hardware switching for IPv6 multicast packets.
uplink	(Optional) Enables IPv6 multicast on the uplink ports of the Supervisor Engine 720-10GE.

Command Default

This command is enabled with the **connected** and **replication-mode ingress** keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXH	This command was modified. The **shared-tree** and the **uplink** keywords were added.
12.2(33)SXI	This command was modified. The **issu-support**keyword was added on the Supervisor Engine 4.

Release	Modification
12.2(33)SXI2	This command was modified. The **issu-support**keyword was added on the Supervisor Engine 720 in distributed Cisco Express Forwarding (dCEF)-only mode.

Usage Guidelines

You must enter the **ipv6 mfib hardware-switching uplink** command to enable IPv6 multicast hardware switching on the standby Supervisor Engine 720-10GE.

Note The system message "PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL" is displayed on the Supervisor Engine if both the **fabric switching-mode allow dcef-only** and **ipv6 mfib hardware-switching uplink** commands are configured. The router will ignore the command configured last.

The **ipv6 mfib hardware-switching uplink** command ensures support of IPv6 multicast on standby uplink ports on systems that are configured with a Supervisor Engine 720-10GE only. You must reboot the system for this command to take effect. The MET space is halved on both the supervisor engines and the C+ modules.

Enabling the ipv6 mfib hardware-switching issu-support command will consume one Switched Port Analyzer (SPAN) session. This command will be effective if the image versions on the active and standby supervisors are different. If the command is not enabled, then the IPv6 multicast traffic ingressing and egressing from standby uplinks will be affected. This command is NVGENed. This command should be configured only once and preferably before performing the In-Service Software Upgrade (ISSU) load version process.

Note After completing the ISSU process, the administrator should disable the configured ipv6 mfib hardware-switching issu-support command.

Examples

The following example shows how to prevent the installation of the subnet entries on a global basis:

```
Router(config)# ipv6 mfib hardware-switching
```

The following example shows how to set the hardware replication mode to ingress:

```
Router(config)# ipv6 mfib hardware-switching replication-mode ingress
```

The following example shows how to enable IPv6 multicast on standby uplink ports on systems that are configured with a Supervisor Engine 720-10GE only:

```
Router(config)# ipv6 mfib hardware-switching uplink
Router(config)# end
Router# reload
```

Related Commands

Command	Description
f abric switching-mode allow dcef-only	Enables the truncated mode in the presence of two or more fabric-enabled switching modules.

Command	Description
show platform software ipv6-multicast	Displays information about the platform software for IPv6 multicast.

ipv6 mfib-mode centralized-only

To disable distributed forwarding on a distributed platform, use the **ipv6 mfib-mode centralized-only** command in global configuration mode. To reenable multicast forwarding, use the **no** form of this command.

ipv6 mfib-mode centralized-only

no ipv6 mfib-mode centralized-only

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast distributed forwarding is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Distributed forwarding is enabled by default when the **ipv6 multicast-routing**, **ipv6 cef distributed**, and the **ipv6 mfib** commands are enabled. The ipv6 mfib-mode centralized-only command disables distributed forwarding. All multicast forwarding is performed centrally.

Examples

The following example reenables distributed forwarding:

```
ipv6 mfib-mode centralized-only
```

ipv6 mld access-group

To perform IPv6 multicast receiver access control, use the **ipv6 mld access-group** command in interface configuration mode. To stop using multicast receiver access control, use the **no** form of this command.

ipv6 mld access-group *access-list-name*

no ipv6 mld access-group *access-list-name*

Syntax Description

access-list-name	A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

Command Default

All groups and sources are allowed.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The ipv6 mld access-group command is used for receiver access control and to check the groups and sources in Multicast Listener Discovery (MLD) reports against the access list. The **ipv6 mld access-group** command also limits the state created by MLD reports. Because Cisco supports MLD version 2, the **ipv6 mld access-group** command allows users to limit the list of groups a receiver can join. You can also use this command to allow or deny sources used to join Source Specific Multicast (SSM) channels.

If a report (S1, S2...Sn, G) is received, the group (0, G) is first checked against the access list. If the group is denied, the entire report is denied. If the report is allowed, each individual (Si, G) is checked against the access list. State is not created for the denied sources.

Examples

The following example creates an access list called acc-grp-1 and denies all the state for group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example creates an access list called acc-grp-1 and permits all the state for only group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example permits only EXCLUDE(G,{}) reports. This example converts EXCLUDE(G,{S1, S2..Sn}) into EXCLUDE(G,{}):

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 host :: host ff04::10
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example filters a particular source 100::1 for a group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 host 100::1 host ff04::10
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

ipv6 mld explicit-tracking

To enable explicit tracking of hosts, use the **ipv6 mld explicit-tracking**command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 mld explicit-tracking *access-list-name*

no ipv6 mld explicit-tracking *access-list-name*

Syntax Description

access-list-name	A standard IPv6 named access list that defines the multicast groups and sources to allow or deny.

Command Default

Explicit tracking is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When explicit tracking is enabled, the fast leave mechanism can be used with Multicast Listener Discovery (MLD) version 2 host reports. The *access-list-name* argument specifies a named IPv6 access list that can be used to specify the group ranges for which a user wants to apply explicit tracking.

Examples

The following example shows how to enable MLD explicit tracking on an access list named list1:

```
ipv6 mld explicit-tracking list1
```

ipv6 mld host-proxy

To enable the Multicast Listener Discovery (MLD) proxy feature, use the **ipv6 mld host-proxy** command in global configuration mode. To disable support for this feature, use the **no** form of this command.

ipv6 mld host-proxy [*group-acl*]

no ipv6 mld host-proxy

Syntax Description

group-acl	(Optional) Group access list (ACL).

Command Default

The MLD proxy feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mld host-proxy** command to enable the MLD proxy feature. If the *group-acl* argument is specified, the MLD proxy feature is supported for the multicast route entries that are permitted by the group ACL. If the *group-acl* argument is not provided, the MLD proxy feature is supported for all multicast routes present in multicast routing table.

Only one group ACL is configured at a time. Users can modify the group ACL by entering this command using a different *group-acl* argument.

Examples

The following example enables the MLD proxy feature for the multicast route entries permitted by the group ACL named "proxy-group":

```
Router(config)# ipv6 mld host-proxy proxy-group
```

Related Commands

Command	Description
ipv6 mld host-proxy interface	Enables the MLD proxy feature on a specified interface on an RP.
show ipv6 mld host-proxy	Displays IPv6 MLD host proxy information.

ipv6 mld host-proxy interface

To enable the Multicast Listener Discovery (MLD) proxy feature on a specified interface on a Route Processor (RP), use the **ipv6 mld host-proxy interface**command in global configuration mode. To disable the MLD proxy feature on a RP, use the **no** form of this command.

ipv6 mld host-proxy interface [*group-acl*]

no ipv6 mld host-proxy interface

Syntax Description

group-acl	(Optional) Group access list (ACL).

Command Default

The MLD proxy feature is not enabled on the RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use the **ipv6 mld host-proxy interface** command to enable the MLD proxy feature on a specified interface on an RP. If a router is acting as an RP for an multicast-route proxy entry, it generates an MLD report on the specified host-proxy interface. Only one interface can be configured as a host-proxy interface, and the host-proxy interface can be modified by using this command with a different interface name.

If a router is not acting as an RP, enabling this command does not have any effect, nor will it generate an error or warning message.

Examples

The following example specifies Ethernet 0/0 as the host-proxy interface:

```
Router (config)# ipv6 mld host-proxy interface Ethernet 0/0
```

Related Commands

Command	Description
ipv6 mld host-proxy	Enables the MLD proxy feature.
show ipv6 mld host-proxy	Displays IPv6 MLD host proxy information.

ipv6 mld join-group

To configure Multicast Listener Discovery (MLD) reporting for a specified group and source, use the **ipv6 mld join-group** command in interface configuration mode. To cancel reporting and leave the group, use the **no** form of this command.

ipv6 mld join-group [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** *acl* }

Syntax Description

group-address	(Optional) IPv6 address of the multicast group.
include	(Optional) Enables include mode.
exclude	(Optional) Enables exclude mode.
source-address	Unicast source address to include or exclude.
source-list	Source list on which MLD reporting is to be configured.
acl	(Optional) Access list used to include or exclude multiple sources for the same group.

Command Default

If a source is specified and no mode is specified, the default is to include the source.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **ipv6 mld join-group** command configures MLD reporting for a specified source and group. The packets that are addressed to a specified group address will be passed up to the client process in the device. The packets will be forwarded out the interface depending on the normal Protocol Independent Multicast (PIM) activity.

The **source-list** keyword and *acl* argument may be used to include or exclude multiple sources for the same group. Each source is included in the access list in the following format:

permit ipv6 host *source* **any**

If the **ipv6 mld join-group**command is repeated for the same group, only the most recent command will take effect. For example, if you enter the following commands, only the second command is saved and will appear in the MLD cache:

```
Device(config-if)# ipv6 mld join-group ff05::10 include 2000::1
Device(config-if)# ipv6 mld join-group ff05::10 include 2000::2
```

Examples

The following example configures MLD reporting for specific groups:

```
Device(config-if)# ipv6 mld join-group ff04::10
```

Related Commands

Command	Description
no ipv6 mld router	Disables MLD router-side processing on a specified interface.

ipv6 mld limit

To limit the number of Multicast Listener Discovery (MLD) states on a per-interface basis, use the **ipv6 mld limit** command in interface configuration mode. To disable a configured MLD state limit, use the **no** form of this command.

ipv6 mld limit *number* [**except** *access-list*]

no ipv6 mld limit *number* [**except** *access-list*]

Syntax Description

number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.
except	(Optional) Excludes an access list from the configured MLD state limit.
access-list	(Optional) Access list to exclude from the configured MLD state limit.

Command Default

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed per interface on a router when you configure this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was modified. It was integrated into Cisco IOS Release 12.2(50)SY.
15.0(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

Use the **ipv6 mld limit**command to configure a limit on the number of MLD states resulting from MLD membership reports on a per-interface basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache, and traffic for the excess membership reports is not forwarded.

Use the **ipv6 mld state-limit** command in global configuration mode to configure the global MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

If you do not configure the **except** *access-list* keyword and argument, all MLD states are counted toward the configured cache limit on an interface. Use the **except** *access-list* keyword and argument to exclude particular groups or channels from counting toward the MLD cache limit. An MLD membership report is counted against the per-interface limit if it is permitted by the extended access list specified by the **except***access-list* keyword and argument.

Examples

The following example shows how to limit the number of MLD membership reports on Ethernet interface 0:

```
interface ethernet 0
 ipv6 mld limit 100
```

The following example shows how to limit the number of MLD membership reports on Ethernet interface 0. In this example, any MLD membership reports from access list cisco1 do not count toward the configured state limit:

```
interface ethernet 0
 ipv6 mld limit 100 except cisco1
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the user to perform IPv6 multicast receiver access control.
ipv6 mld state-limit	Limits the number of MLD states on a global basis.

ipv6 mld query-interval

To configure the frequency at which the Cisco IOS software sends Multicast Listener Discovery (MLD) host-query messages, use the **ipv6 mld query-interval** command in interface configuration mode. To return to the default frequency, use the **no** form of this command.

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

Syntax Description

seconds	Frequency, in seconds, at which to send MLD host-query messages. It can be a number from 0 to 65535. The default is 125 seconds.

Command Default

The default is 125 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the router's attached networks. Hosts respond with MLD report messages indicating

that they want to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group).

The designated router for a LAN is the only router that sends MLD host-query messages.

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command**should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-max-response-time** and **ipv6 mld query-timeout** commands. If you change the default value for the **ipv6 mld query-interval** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example sets the MLD query interval to 60 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-interval 60
```

Related Commands

Command	Description
ipv6 mld query-max- response-time	Configures the maximum response time advertised in MLD queries.
ipv6 mld query-timeout	Configures the timeout value before the router takes over as the querier for the interface.
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.
show ipv6 mld groups	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

ipv6 mld query-max-response-time

To configure the maximum response time advertised in Multicast Listener Discovery (MLD) queries, use the **ipv6 mld query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

Syntax Description

seconds	Maximum response time, in seconds, advertised in MLD queries. The default value is 10 seconds.

Command Default

The default is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

Note If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command**should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval**and **ipv6 mld query-timeout** commands. If you change the default value for the **ipv6 mld query-max-response-time** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example configures a maximum response time of 20 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-max-response-time 20
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 mld query-timeout	Configures the timeout value before the router takes over as the querier for the interface.
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.
show ipv6 mld groups	Displays the multicast groups that are directly connected to the router and that were learned through MLD.

ipv6 mld query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the **ipv6 mld query-timeout**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-timeout *seconds*

no ipv6 mld query-timeout

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier.

Command Default

The default is 250 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The query interval is calculated as query timeout = (2 x query interval) + query-max-response-time / 2. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time**

command is configured to be 20 seconds, then the **ipv6 mld query-timeout command**should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval**and **ipv6 mld query-max-response-time**commands. If you change the default value for the **ipv6 mld query-timeout** command, make sure the changed value works correctly with these two commands.

Caution Changing the default value may severely impact multicast forwarding.

Examples

The following example configures the router to wait 130 seconds from the time it received the last query before it takes over as the querier for the interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-timeout 130
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 mld query-max- response-time	Configures the maximum response time advertised in MLD queries.

ipv6 mld router

To enable Multicast Listener Discovery (MLD) group membership message processing and routing on a specified interface, use the **ipv6 mld router**command in interface configuration mode. To disable MLD group membership message processing and routing on a specified interface, use the **no** form of the command.

ipv6 mld router

no ipv6 mld router

Syntax Description

This command has no arguments or keywords.

Command Default

MLD message processing and egress routing of multicast packets is enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

When the **ipv6 multicast-routing**commandis configured, MLD group membership message processing is enabled on every interface. The **no ipv6 mld router** command prevents forwarding (routing) of multicast packets to the specified interface and disables static multicast group configuration on the specified interface.

The **no ipv6 mld router** command also disables MLD group membership message processing on a specified interface. When MLD group membership message processing is disabled, the router stops sending MLD queries and stops keeping track of MLD members on the LAN.

If the **ipv6 mld join-group** command is also configured on an interface, it will continue with MLD host functionality and will report group membership when an MLD query is received.

MLD group membership processing is enabled by default. The **ipv6 multicast-routing**command does not enable or disable MLD group membership message processing.

Examples

The following example disables MLD group membership message processing on an interface and disables routing of multicast packets to that interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mld router
```

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

ipv6 mld snooping

no ipv6 mld snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping explicit-tracking

To enable explicit host tracking, use the **ipv6 mld snooping explicit-tracking** command in interface configuration mode. To disable explicit host tracking, use the **no** form of this command.

ipv6 mld snooping explicit-tracking

no ipv6 mld snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit host tracking is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Explicit host tracking is supported only with Internet Group Management Protocol Version 3 (IGMPv3) hosts.

When you enable explicit host tracking and the Cisco 7600 series router is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Cisco 7600 series router forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the Cisco 7600 series router does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Cisco 7600 series router works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that are reported by the host.

- The list of sources for each group that are reported by the hosts.
- The router filter mode of each group.
- The list of hosts for each group that request the source.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping explicit-tracking
```

Related Commands

Command	Description
ipv6 mld snooping limit	Configures the MLDv2 limits.
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping last-member-query-interval

To configure the last member query interval for Multicast Listener Discovery Version 2 (MLDv2) snooping, use the **ipv6 mld snooping last-member-query-interval** command in interface configuration. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping last-member-query-interval *interval*

no ipv6 mld snooping last-member-query-interval

Syntax Description

interval	Interval for the last member query; valid values are from 100 to 900 milliseconds in multiples of 100 milliseconds.

Command Default

The default is 1000 milliseconds (1 second).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Cisco 7600 series router waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no ipv6 mld snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes a higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ipv6 mld snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last member query interval to 200 milliseconds:

```
Router(config-if)#
ipv6 mld snooping last-member-query-interval 200
Router(config-if)#
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping limit

To configure Multicast Listener Discovery version 2 (MLDv2) protocol limits, use the **ipv6 mld snooping limit**command in global configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 mld snooping limit {**l2-entry-limit** *max-entries*| **rate** *pps*| **track** *max-entries*}

no ipv6 mld snooping limit {**l2-entry-limit**| **rate**| **track**}

Syntax Description

l2-entry-limit *max-entries*	Specifies the maximum number of Layer 2 entries that can be installed by MLD snooping. Valid values are from 1 to 100000 entries.
rate *pps*	Specifies the rate limit of incoming MLDv2 messages. Valid values are from 100 to 6000 packets per second (pps).
track *max-entries*	Specifies the maximum number of entries in the explicit-tracking database. Valid values are from 0 to 128000 entries.

Command Default

The *max-entries*argument default is 32000 .

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 .

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* argument to 0, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries* value, a system logging message is generated.

When you reduce the *max-entries*argument, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to set the maximum number of Layer 2 entries that can be installed by MLD snooping:

```
Router(config)#
 ipv6 mld snooping limit l2-entry-limit 100000
```

This example shows how to set the rate limit for incoming MLDv2-snooping packets:

```
Router(config)#
 ipv6 mld snooping limit rate 200
```

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)#
 ipv6 mld snooping limit track 20000
```

This example shows how to disable software rate limiting:

```
Router(config)#
 no ipv6 mld snooping limit rate
```

Related Commands

Command	Description
ipv6 mld snooping explicit tracking	Enables explicit host tracking.

ipv6 mld snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ipv6 mld snooping mrouter** command in interface configuration mode.

ipv6 mld snooping mrouter interface *type slot/port*

Syntax Description

interface *type*	Specifies the interface type: valid values are **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**
slot / *port*	Module and port number. The slash mark is required.

Command Default

No defaults are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure a Layer 2 port as a multicast router port:

```
Router(config-if)# ipv6 mld snooping mrouter interface fastethernet 5/6
```

Related Commands

Command	Description
mac-address-table static	Adds static entries to the MAC address table.
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping querier

To enable the Multicast Listener Discovery version 2 (MLDv2) snooping querier, use the **ipv6 mld snooping querier** command in interface configuration mode. To disable the MLDv2 snooping querier, use the **no** form of this command.

ipv6 mld snooping querier

no ipv6 mld snooping querier

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must configure an IPv6 address on the VLAN interface. When this feature is enabled, the MLDv2 snooping querier uses the IPv6 address as the query source address.

If there is no IPv6 address configured on the VLAN interface, the MLDv2 snooping querier does not start. The MLDv2 snooping querier disables itself if the IPv6 address is cleared. When this feature is enabled, the MLDv2 snooping querier restarts if you configure an IPv6 address.

The MLDv2 snooping querier:

- Does not start if it detects MLDv2 traffic from an IPv6 multicast router.
- Starts after 60 seconds if it detects no MLDv2 traffic from an IPv6 multicast router.
- Disables itself if it detects MLDv2 traffic from an IPv6 multicast router.

You can enable the MLDv2 snooping querier on all the Catalyst 6500 series switches in the VLAN that support it. One switch is elected as the querier.

Examples

This example shows how to enable the MLDv2 snooping querier on VLAN 200:

```
Router(config)# interface vlan 200
Router(config-if)# ipv6 mld snooping querier
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping report-suppression

To enable Multicast Listener Discovery version 2 (MLDv2) report suppression on a VLAN, use the **ipv6 mld snooping report-suppression** command in interface configuration mode. To disable report suppression on a VLAN, use the **no** form of this command.

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enable explicit tracking before enabling report suppression.

This command is supported on VLAN interfaces only.

Examples

This example shows how to enable explicit host tracking:

```
Router(config-if)# ipv6 mld snooping report-suppression
```

ipv6 mld ssm-map enable

To enable the Source Specific Multicast (SSM) mapping feature for groups in the configured SSM range, use the **ipv6 mld ssm-map enable**command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**

no ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**

Syntax Description

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

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The **ipv6 mld ssm-map enable**command enables the SSM mapping feature for groups in the configured SSM range. When the **ipv6 mld ssm-map enable**command is used, SSM mapping defaults to use the Domain Name System (DNS).

SSM mapping is applied only to received Multicast Listener Discovery (MLD) version 1 or MLD version 2 membership reports.

Examples

The following example shows how to enable the SSM mapping feature:

```
Router(config)# ipv6 mld ssm-map enable
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map query dns

To enable Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ipv6 mld ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map query dns**

no ipv6 mld [**vrf** *vrf-name*] **ssm-map query dns**

Syntax Description

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

Command Default

DNS-based SSM mapping is enabled by default when the SSM mapping feature is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

DNS-based SSM mapping is enabled by default when the SSM mapping feature is enabled using the **ipv6 mld ssm-map enable** command. If DNS-based SSM mapping is disabled by entering the **no** version of the **ipv6 mld ssm-map query dns** command, only statically mapped SSM sources configured by the **ipv6 mld ssm-map static** command will be determined.

For DNS-based SSM mapping to succeed, the router needs to find at least one correctly configured DNS server.

Examples

The following example enables the DNS-based SSM mapping feature:

```
ipv6 mld ssm-map query dns
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map static

To configure static Source Specific Multicast (SSM) mappings, use the **ipv6 mld ssm-map static**command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*

no ipv6 mld [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of the IPv6 access list that identifies a group range. Access list names cannot contain a space or quotation mark, or begin with a numeric.
source-address	Source address associated with an MLD membership for a group identified by the access list.

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **ipv6 mld ssm-map static** command to configure static SSM mappings. If SSM mapping is enabled and the router receives a Multicast Listener Discovery (MLD) membership for group G in the SSM range, the router tries to determine the source addresses associated with G by checking the **ipv6 mld ssm-map static** command configurations.

If group G is permitted by the access list identified by the *access-list* argument, then the specified source address is used. If multiple static SSM mappings have been configured using the **ipv6 mld ssm-map static** command and G is permitted by multiple access lists, then the source addresses of all matching access lists will be used (the limit is 20).

If no static SSM mappings in the specified access lists match the MLD membership, SSM mapping queries the Domain Name System (DNS) for address mapping.

Examples

The following example enables the SSM mapping feature and configures the groups identified in the access list named SSM_MAP_ACL_2 to use source addresses 2001:0DB8:1::1 and 2001:0DB8:1::3:

```
ipv6 mld ssm-map enable
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::1
ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::3
ipv6 mld ssm-map query dns
```

Related Commands

Command	Description
debug ipv6 mld ssm-map	Displays debug messages for SSM mapping.
ipv6 mld ssm-map enable	Enables the SSM mapping feature for groups in the configured SSM range.
ipv6 mld ssm-map query dns	Enables DNS-based SSM mapping.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld state-limit

To limit the number of Multicast Listener Discovery (MLD) states globally, use the **ipv6 mld state-limit** command in global configuration mode. To disable a configured MLD state limit, use the **no** form of this command.

ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*

no ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
number	Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.

Command Default

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed globally on a router when you configure this command.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(50)SY	This command was modified. It was integrated into Cisco IOS Release 12.2(50)SY.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **ipv6 mld state-limit** command to configure a limit on the number of MLD states resulting from MLD membership reports on a global basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache and traffic for the excess membership reports is not forwarded.

Use the **ipv6 mld limit** command in interface configuration mode to configure the per-interface MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

Examples

The following example shows how to limit the number of MLD states on a router to 300:

```
ipv6 mld state-limit 300
```

Related Commands

Command	Description
ipv6 mld access-group	Enables the performance of IPv6 multicast receiver access control.
ipv6 mld limit	Limits the number of MLD states resulting from MLD membership state on a per-interface basis.

ipv6 mld static-group

To statically forward traffic for the multicast group onto a specified interface and cause the interface to behave as if a Multicast Listener Discovery (MLD) joiner were present on the interface, use the **ipv6 mld static-group** command in interface configuration mode. To stop statically forwarding traffic for the specific multicast group, use the **no** form of this command.

ipv6 mld join-group [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** *acl* }

Syntax Description

group-address	(Optional) IPv6 address of the multicast group.
include	(Optional) Enables include mode.
exclude	(Optional) Enables exclude mode.
source-address	Unicast source address to include or exclude.
source-list	Source list on which MLD reporting is to be configured.
acl	(Optional) Access list used to include or exclude multiple sources for the same group.

Command Default

If no mode is specified for the source, use of the **include** keyword is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

The ipv6 multicast-routing command must be configured for the **ipv6 mld static-group**command to be effective.

When the **ipv6 mld static-group** command is enabled, packets to the group are either fast-switched or hardware-switched, depending on the platform. Unlike what happens when using the **ipv6 mld join-group** command, a copy of the packet is not sent to the process level.

An access list can be specified to include or exclude multiple sources for the same group. Each source is included in the access list in the following format:

permit ipv6 host *source* **any**

Note Using the **ipv6 mld static-group** command is not sufficient to allow traffic to be forwarded onto the interface. Other conditions, such as the absence of a route, the router not being the designated router, or losing an assert, can cause the router not to forward traffic even if the **ipv6 mld static-group**command is configured.

Examples

The following example statically forward traffic for the multicast group onto the specified interface:

```
ipv6 mld static-group ff04::10 include 100::1
```

Related Commands

Command	Description
ipv6 mld join-group	Configures MLD reporting for a specified group and source.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.
no ipv6 pim	Use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface.