ip rgmp through ipv6 multicast-routing

ip rgmp

To enable the Router-Port Group Management Protocol (RGMP) on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, use the **ip rgmp**command in interface configuration mode. To disable RGMP on the interfaces, use the **no** form of this command.

ip rgmp
no ip rgmp

Syntax Description

This command has no arguments or keywords.

Command Default

RGMP is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)S	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

RGMP is supported only on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.

Before you enable RGMP, the following features must be enabled on your router:

- IP routing
- IP multicast
- PIM in sparse mode, sparse-dense mode, source specific mode, or bidirectional mode

If your router is in a bidirectional group, make sure to enable RGMP only on interfaces that do not function as a designated forwarder (DF). If you enable RGMP on an interface that functions as a DF, the interface will not forward multicast packets up the bidirectional shared tree to the rendezvous point (RP).

The following features must be enabled on your switch:

- IP multicast
- IGMP snooping

Examples

The following example enables RGMP on Ethernet interface 1/0:

```
interface ethernet 1/0
 ip rgmp
```

Related Commands

Command	Description
debug ip rgmp	Logs debug messages sent by an RGMP-enabled router.
show ip igmp interface	Displays multicast-related information about an interface.

ip sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the **ip sap cache-timeout**command in global configuration mode. To restore the default value, use the **no** form of this command.

ip sap cache-timeout *minutes*
no ip sap cache-timeout

Syntax Description

minutes	Time (in minutes) that a SAP cache entry is active in the cache.

Command Default

By default, session announcements remain for 1440 minutes (24 hours) in the cache.

Command Modes

Global configuration

Command History

Release	Modification
11.2	The **ip sdr cache-timeout** command was introduced.
12.2	The **ip sdr cache-timeout** command was replaced by the **ip sap cache-timeout**command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines how long session announcements are cached by the router. Active session announcements are periodically re-sent by the originating site, refreshing the cached state in the router. The minimum interval between announcements for a single group is 5 minutes. Setting the cache timeout to a value less than 30 minutes is not recommended. Set the cache timeout to 0 to keep entries in the cache indefinitely.

Examples

The following example causes SAP cache entries to remain in the cache for 30 minutes:

```
ip sap cache-timeout 30
```

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
show ip sap	Displays the SAP cache.

ip sap listen

To enable the Cisco IOS software to listen to session directory announcements, use the **ip sap listen**command in interface configuration mode. To disable the function, use the **no** form of this command.

ip sap listen
no ip sap listen

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	The **ip sdr listen** command was introduced.
12.2	The **ip sdr listen**command was replaced by the **ip sap listen**command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco IOS software can receive and store Session Description Protocol (SDP) and Session Announcement Protocol (SAP) session announcements. When the **ip sap listen** command is configured on an interface, the well-known session directory groups on that interface can receive and store session announcements. The announcements can be displayed with the **show ip sap** command. The **ip multicast rate-limit** command uses stored session announcements. To configure the period of time after which received announcements will expire, use the **ip sap cache-timeout** command.

When the **no ip multicast routing** command is configured, announcements are only stored if they are received on an interface configured with the **ip sap listen** command. When a system is configured as a multicast router, it is sufficient to configure the **ip sap listen** command on only a single multicast-enabled interface. The well-known session directory groups are handled as local joined groups after the **ip sap listen** command is first configured (see the L flag of the **show ip mroute**command). This configuration causes announcements received from all multicast-enabled interfaces to be routed and stored within the system.

Examples

The following example shows how to enable a router to listen to session directory announcements:

```
ip routing
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.

Command	Description
ip multicast rate-limit	Controls the rate a sender from the source list can send to a multicast group in the group list.
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip sap cache-timeout	Limits how long a SAP cache entry stays active in the cache.
show ip mroute	Displays the contents of the IP mroute routing table.
show ip sap	Displays the SAP cache.

ip sdr cache-timeout

The **ip sdr cache-timeout** command is replaced by the **ip sap cache-timeout** command. See the description of the **ip sap cache-timeout** command for more information.

ip sdr listen

The **ip sdr listen**command is replaced by the **ip sap listen** command. See the description of the **ip sap listen** command for more information.

ip service reflect

To match and rewrite multicast packets routed onto a Vif1 interface, use the **ip service reflect** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address* **mask-len** *number* **source** *new-source-address*
no ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address* **mask-len** *number* **source** *new-source-address*

Syntax Description

input-interface	Interface type and number.
destination	Identifies packets with the specified destination address.
destination-address	Destination IP address in the packets, in A.B.C.D format.
to	Modifies the destination IP address in reflected packets to a new IP address.
new-destination-address	New destination address to be used, in A.B.C.D format.
mask-len *number*	Specifies the mask length of the destination address to match. The *number* argument is a value from 0 to 32.
source	Modifies the source address in reflected packets. The source address must be on the same subnet as the Vif1 interface.
new-source-address	New source address to be used, in A.B.C.D format.

Command Default

The multicast service reflection feature is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **ip service reflect** command to match and rewrite multicast packets routed onto a Vif1 interface.

The matched and rewritten packet is sent back into Cisco multicast packet routing, where it is handled like any other packet arriving from an interface.

More than one multicast service reflection operation can be configured to match the same packet, allowing you to replicate the same received traffic to multiple destination addresses.

Examples

The following example shows how to translate any multicast packet with a destination address of 239.1.1.0/24 to a destination of 239.2.2.0/24 with a new source address of 10.1.1.2. For example, a

packet with a source and destination of (10.10.10.10, 239.1.1.15) would be translated to (10.1.1.2, 239.2.2.15).

```
Router(config)# interface Vif1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip service reflect Ethernet 0/0 destination 239.1.1.0 to 239.2.2.0
mask-len 24 source 10.1.1.2
Router(config-if)# ip igmp static-group 239.1.1.0
Router(config-if)# ip igmp static-group 239.1.1.1
```

ip urd

To enable interception of TCP packets sent to the reserved URL Rendezvous Directory (URD) port 465 on an interface and processing of URD channel subscription reports, use the **ip urd** command in interface configuration mode. To disable URD on an interface, use the **no** form of this command.

ip urd [**proxy**]
no ip urd [**proxy**]

Syntax Description

proxy	(Optional) Allows an interface to accept URL requests from any TCP connection sent to that interface. If the **proxy** keyword is not configured, the interface will accept URL requests from TCP connections only if the requests originated from directly connected hosts. The **proxy** option must be enabled on an interface if it is unnumbered or if it has downstream routers configured with Internet Group Management Protocol (IGMP) proxy routing. To prevent users on the backbone from creating URD state on your router, do not enable the **proxy** option on a backbone interface of your router.

Command Default

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To use this command, you must first define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When URD is enabled, it is supported in the SSM range of addresses only. We recommend that you not enable URD on backbone interfaces, but only on interfaces connecting to hosts.

URD functionality is available for multicast process switching, fast switching, and distributed fast-switching paths.

Examples

The following example shows how to configure URD on Ethernet interface 3/3:

```
interface ethernet 3/3
 ip urd
```

Related Commands

Command	Description
ip pim ssm	Defines the SSM range of IP multicast addresses.

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 output

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

ipv6 mfib cef output
no ipv6 mfib cef output

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipv6 mfib fast

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

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

ipv6 mfib fast
no ipv6 mfib fast

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipv6 mfib forwarding

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

ipv6 mfib forwarding
no ipv6 mfib forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipv6 mfib hardware-switching

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXH	This command was modified. The **shared-tree** and the **uplink** keywords were added.
12.2(33)SXI	This command was modified. The **issu-support**keyword was added on the Supervisor Engine 4.
12.2(33)SXI2	This command was modified. The **issu-support**keyword was added on the Supervisor Engine 720 in distributed Cisco Express Forwarding (dCEF)-only mode.

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

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

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

Related Commands

Command	Description
f abric switching-mode allow dcef-only	Enables the truncated mode in the presence of two or more fabric-enabled switching modules.
show platform software ipv6-multicast	Displays information about the platform software for IPv6 multicast.

ipv6 mfib-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-mode centralized-only

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

ipv6 mfib-mode centralized-only
no ipv6 mfib-mode centralized-only

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast distributed forwarding is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example reenables distributed forwarding:

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

ipv6 mld access-group

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

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

Syntax Description

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

Command Default

All groups and sources are allowed.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
```

```
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

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

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

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

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

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

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

ipv6 mld explicit-tracking

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

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

Syntax Description

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

Command Default

Explicit tracking is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

ipv6 mld host-proxy

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

ipv6 mld host-proxy [*group-acl*]
no ipv6 mld host-proxy

Syntax Description

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

Command Default

The MLD proxy feature is not enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipv6 mld host-proxy interface

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

ipv6 mld host-proxy interface [*group-acl*]
no ipv6 mld host-proxy interface

Syntax Description

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

Command Default

The MLD proxy feature is not enabled on the RP.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ipv6 mld join-group

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

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

permit ipv6 host *source* **any**

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

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

Examples

The following example configures MLD reporting for specific groups:

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

Related Commands

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

ipv6 mld limit

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

the per-interface limit if it is permitted by the extended access list specified by the **except***access-list* keyword and argument.

Examples

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

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

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

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

Related Commands

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

ipv6 mld query-interval

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

ipv6 mld query-interval *seconds*
no ipv6 mld query-interval

Syntax Description

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

Command Default

The default is 125 seconds.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the router's attached networks. Hosts respond with MLD report messages indicating that they want to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group).

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

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

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

Caution Changing the default value may severely impact multicast forwarding.

Examples

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

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

Related Commands

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

ipv6 mld query-max-response-time

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

ipv6 mld query-max-response-time *seconds*
no ipv6 mld query-max-response-time

Syntax Description

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

Command Default

The default is 10 seconds.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Caution Changing the default value may severely impact multicast forwarding.

Examples

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

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

Related Commands

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

ipv6 mld query-timeout

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

ipv6 mld query-timeout *seconds*
no ipv6 mld query-timeout

Syntax Description

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

Command Default

The default is 250 seconds.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Caution Changing the default value may severely impact multicast forwarding.

Examples

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

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

Related Commands

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

ipv6 mld router

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

ipv6 mld router
no ipv6 mld router

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

ipv6 mld snooping

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

ipv6 mld snooping
no ipv6 mld snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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

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

Examples

This example shows how to enable MLDv2 snooping globally:

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

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping explicit-tracking

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

ipv6 mld snooping explicit-tracking
no ipv6 mld snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit host tracking is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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

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

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

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

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

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

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

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

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

Examples

This example shows how to enable explicit host tracking:

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

Related Commands

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

ipv6 mld snooping last-member-query-interval

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

ipv6 mld snooping last-member-query-interval *interval*
no ipv6 mld snooping last-member-query-interval

Syntax Description

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

Command Default

The default is 1000 milliseconds (1 second).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping limit

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

ipv6 mld snooping limit l2-entry-limit *max-entries* | **rate** *pps* | **track** *max-entries*
no ipv6 mld snooping limit l2-entry-limit | **rate** | **track**

Syntax Description

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

Command Default

The *max-entries*argument default is 32000 .

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

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

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

This example shows how to disable software rate limiting:

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

Related Commands

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

ipv6 mld snooping mrouter

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

ipv6 mld snooping mrouter interface *type slot/port*

Syntax Description

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

Command Default

No defaults are configured.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

ipv6 mld snooping querier

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

ipv6 mld snooping querier
no ipv6 mld snooping querier

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

The MLDv2 snooping querier:

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

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

Examples

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

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

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 mld snooping report-suppression

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

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You must enable explicit tracking before enabling report suppression.

This command is supported on VLAN interfaces only.

Examples

This example shows how to enable explicit host tracking:

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

ipv6 mld ssm-map enable

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

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

Syntax Description

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

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

Command	Description
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map query dns

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

Command	Description
ipv6 mld ssm-map static	Configures static SSM mappings.
show ipv6 mld ssm-map	Displays SSM mapping information.

ipv6 mld ssm-map static

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

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

Syntax Description

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

Command Default

The SSM mapping feature is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipv6 mld state-limit

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ipv6 mld static-group

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

permit ipv6 host *source* **any**

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

Examples

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

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

Related Commands

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

ipv6 multicast aaa account receive

To enable authentication, authorization, and accounting (AAA) accounting on specified groups or channels, use the **ipv6 multicast aaa account receive**command in interface configuration mode. To disable AAA accounting, use the **no** form of this command.

ipv6 multicast aaa account receive *access-list-name* [**throttle** *throttle-number*]
no ipv6 multicast aaa account receive

Syntax Description

access-list-name	Access list to specify which groups or channels are to have AAA accounting enabled.
throttle	(Optional) Limits the number of records sent during channel surfing. No record is sent if a channel is viewed for less than a specified, configurable period of time.
throttle-number	(Optional) Throttle or surfing interval, in seconds.

Command Default

No AAA accounting is performed on any groups or channels.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Use the **ipv6 multicast aaa account receive**command to enable AAA accounting on specific groups or channels and to set throttle interval limits on records sent during channel surfing.

Examples

The following example enables AAA accounting using an access list named list1:

```
Router(config-if)# ipv6 multicast aaa account receive list1
```

Related Commands

Command	Description
aaa accounting multicast default	Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.

ipv6 multicast boundary

To configure an IPv6 multicast boundary on the interface for a specified scope, use the **ipv6 multicast boundary** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 multicast boundary block source
no ipv6 multicast boundary block source
ipv6 multicast boundary scope *scope-value*
no ipv6 multicast boundary scope *scope-value*

Syntax Description

block source	Blocks the source of all incoming multicast traffic on an interface.
scope *scope-value*	Specifies the boundary for a particular scope. The scope value can be one of the following: • Link-local address • Subnet-local address • Admin-local address • Site-local address • Organization-local • Virtual Private Network (VPN) • Scope number, which is from 2 through 15

Command Default

Multicast boundary is not configured on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS 12.3(14)T	This command was introduced.
Cisco IOS 12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE 3.13S	This command was modified. The **block** and **source** keywords were added.

Usage Guidelines

Use the **ipv6 multicast boundary block source** command to block all incoming multicast traffic on an interface. However, this command allows the multicast traffic to flow out on the interface and allows any reserved multicast packets to flow in on the interface. This command is primarily used at first-hop routers to prevent local hosts from functioning as multicast sources.

If the **ipv6 multicast boundary scope** command is configured for a particular scope on the Reverse Path Forwarding (RPF) interface, then packets are not accepted on that interface for groups that belong to scopes that are less than or equal to the one that is configured. Protocol Independent Multicast (PIM) join/prune messages for those groups are not sent on the RPF interface. The effect of the scope is verified by checking

the output of the **show ipv6 mrib route** command. The output does not show the RPF interface with Accept flag.

If the **ipv6 multicast boundary scope** command is configured for a particular scope on an interface in the outgoing interface list, packets are not forwarded for groups that belong to scopes that are less than or equal to the one configured.

Protocol Independent Multicast (PIM) join/prune (J/P) messages are not processed when it is received on the interface for groups that belong to scopes that are less than or equal to the one configured. Registers and bootstrap router (BSR) messages are also filtered on the boundary.

Examples

The following example shows how to block the source of all incoming multicast traffic on the interface:

```
Device> enable
Device# configure terminal
Device(config)# int GigabitEthernet0/0/0
Device(config-if)# ipv6 multicast boundary block source
```

The following example sets the scope value to be a scope number of 6:

```
ipv6 multicast boundary scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router to be a candidate BSR.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
show ipv6 mrib route	Displays the MRIB route information.

ipv6 multicast group-range

To disable multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router, use the **ipv6 multicast group-range**command in global configuration mode. To return to the command's default settings, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]
no ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list-name	(Optional) Name of an access list that contains authenticated subscriber groups and authorized channels that can send traffic to the router.

Command Default

Multicast is enabled for groups and channels permitted by a specified access list and disabled for groups and channels denied by a specified access list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 multicast group-range** command provides an access control mechanism for IPv6 multicast edge routing. The access list specified by the *access-list-name* argument specifies the multicast groups or channels that are to be permitted or denied. For denied groups or channels, the router ignores protocol traffic and actions (for example, no Multicast Listener Discovery (MLD) states are created, no mroute states are created, no Protocol Independent Multicast (PIM) joins are forwarded), and drops data traffic on all interfaces in the system, thus disabling multicast for denied groups or channels.

Using the **ipv6 multicast group-range** global configuration command is equivalent to configuring the MLD access control and multicast boundary commands on all interfaces in the system. However, the **ipv6 multicast group-range** command can be overridden on selected interfaces by using the following interface configuration commands:

- **ipv6 mld access-group** *access-list-name*
- **ipv6 multicast boundary scope** *scope-value*

Because the **no ipv6 multicast group-range** command returns the router to its default configuration, existing multicast deployments are not broken.

Examples

The following example ensures that the router disables multicast for groups or channels denied by an access list named list2:

```
Router(config)# ipv6 multicast group-range list2
```

The following example shows that the command in the previous example is overridden on an interface specified by int2:

```
Router(config)# interface int2
Router(config-if)# ipv6 mld access-group int-list2
```

On int2, MLD states are created for groups or channels permitted by int-list2 but are not created for groups or channels denied by int-list2. On all other interfaces, the access-list named list2 is used for access control.

In this example, list2 can be specified to deny all or most multicast groups or channels, and int-list2 can be specified to permit authorized groups or channels only for interface int2.

Related Commands

Command	Description
ipv6 mld access-group	Performs IPv6 multicast receiver access control.
ipv6 multicast boundary scope	Configures a multicast boundary on the interface for a specified scope.

ipv6 multicast limit

To configure per-interface multicast route (mroute) state limiters in IPv6, use the **ipv6 multicast limit** command in interface configuration mode. To remove the limit imposed by a per-interface mroute state limiter, use the **no** form of this command.

ipv6 multicast limit [**connected** | **rpf** | **out**] *limit-acl max* [**threshold** *threshold-value*]
no ipv6 multicast limit [**connected** | **rpf** | **out**] *limit-acl max* [**threshold** *threshold-value*]

Syntax Description

connected	(Optional) Limits mroute states created for an Access Control List (ACL)-classified set of multicast traffic on an incoming (Reverse Path Forwarding [RPF]) interface that is directly connected to a multicast source by counting each time that an mroute permitted by the ACL is created or deleted.
rpf	(Optional) Limits the number of mroute states created for an ACL-classified set of multicast traffic on an incoming (RPF) interface by counting each time an mroute permitted by the ACL is created or deleted.
out	(Optional) Limits mroute outgoing interface list membership on an outgoing interface for an ACL-classified set of multicast traffic by counting each time that an mroute list member permitted by the ACL is added or removed.
limit-acl	Name identifying the ACL that defines the set of multicast traffic to be applied to a per-interface mroute state limiter.
max	Maximum number of mroutes permitted by the per interface mroute state limiter. The range is from 0 to 2147483647.
threshold	(Optional) The mCAC threshold percentage.
threshold-value	(Optional) The specified percentage. The threshold notification default is 0%, meaning that threshold notification is disabled.

Command Default

No per-interface mroute state limiters are configured. Threshold notification is set to 0%; that is, it is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **ipv6 multicast limit** command to configure mroute state limiters on an interface.

For the required *limit-acl* argument, specify the ACL that defines the IPv6 multicast traffic to be limited on an interface. A standard or extended ACL can be specified.

The **ipv6 multicast limit cost**command complements the per-interface **ipv6 multicast limit**command. Once the *limit-acl* argument is matched in the **ipv6 multicast limit**command, the *access-list* argument in the **ipv6**

multicast limit costcommand is checked to see which cost to apply to limited groups. If no cost match is found, the default cost is 1.

The threshold notification for mCAC limit feature notifies the user when actual simultaneous multicast channel numbers exceeds or fall below a specified threshold percentage.

Examples

The following example configures the interface limit on the source router's outgoing interface Ethernet 1/3:

```
interface Ethernet1/3
ipv6 address FE80::40:1:3 link-local
 ipv6 address 2001:0DB8:1:1:3/64
 ipv6 multicast limit out acl1 10
```

Related Commands

Command	Description
ipv6 multicast limit cost	Applies a cost to mroutes that match per-interface mroute state limiters in IPv6.
ipv6 multicast limit rate	Configures the maximum allowed state on the source router.

ipv6 multicast limit cost

To apply a cost to mroutes that match per-interface mroute state limiters in IPv6, use t**he ipv6 multicast limit cost** command in global configuration mode. To restore the default cost for mroutes being limited by per-interface mroute state limiters, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*
no ipv6 multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Access Control List (ACL) name that defines the mroutes for which to apply a cost.
cost-multiplier	Cost value applied to mroutes that match the corresponding ACL. The range is from 0 to 2147483647.

Command Default

If the **ipv6 multicast limit cost** command is not configured or if an mroute that is being limited by a per-interface mroute state limiter does not match any of the ACLs applied to **ipv6 multicast limit cost**command configurations, a cost of 1 is applied to the mroutes being limited.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 multicast limit cost**command to apply a cost to mroutes that match per-interface mroute state limiters (configured with the **ipv6 multicast limit** command in interface configuration mode). This command is primarily used to provide bandwidth-based Call Admission Control (CAC) in network environments where multicast flows utilize different amounts of bandwidth. Accordingly, when this command is configured, the configuration is usually referred to as a bandwidth-based multicast CAC policy.

The **ipv6 multicast limit cost**command complements the per-interface **ipv6 multicast limit**command. Once the *limit-acl* argument is matched in the **ipv6 multicast limit**command, the *access-list* argument in the **ipv6 multicast limit cost**command is checked to see which cost to apply to limited groups. If no cost match is found, the default cost is 1.

Examples

The following example configures the global limit on the source router.

```
Router(config)# ipv6 multicast limit cost costlist1 2
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.

ipv6 multicast limit rate

To configure the maximum allowed state globally on the source router, use the **ipv6 multicast limit rate**command in global configuration mode. To remove the rate value, use the **no** form of this command.

ipv6 multicast limit rate *rate-value*
no ipv6 multicast limit rate *rate-value*

Syntax Description

rate-value	The maximum allowed state on the source router. The range is from 0 through 100.

Command Default

The maximum state is 1.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The ipv6 multicast rate limit command is set to a maximum state of 1 message per second. If the default is set to 0, the syslog notification rate limiter is disabled.

Examples

The following example configures the maximum state on the source router:

```
ipv6 multicast limit rate 2
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.

ipv6 multicast multipath

To enable load splitting of IPv6 multicast traffic across multiple equal-cost paths, use the **ipv6 multicast multipath**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **multipath**
no ipv6 multicast [**vrf** *vrf-name*] **multipath**

Syntax Description

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

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 multicast multipath** command is enabled by default. In the default scenario, the reverse path forwarding (RPF) neighbor is selected randomly from the available equal-cost RPF neighbors, resulting in the load splitting of traffic from different sources among the available equal cost paths. All traffic from a single source is still received from a single neighbor.

When the **no ipv6 multicast multipath** command is configured, the RPF neighbor with the highest IPv6 address is chosen for all sources with the same prefix, even when there are other available equal-cost paths.

Because the **ipv6 multicast multipath**command changes the way an RPF neighbor is selected, it must be configured consistently on all routers in a redundant topology to avoid looping.

Examples

The following example enables load splitting of IPv6 traffic:

```
Router(config)# ipv6 multicast multipath
```

Related Commands

Command	Description
show ipv6 rpf	Checks RPF information for a given unicast host address and prefix.

ipv6 multicast pim-passive-enable

To enable the Protocol Independent Multicast (PIM) passive feature on an IPv6 router, use the **ipv6 multicast pim-passive-enable**command in global configuration mode. To disable this feature, use the **no** form of this command.

ipv6 multicast pim-passive-enable
no ipv6 multicast pim-passive-enable

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **ipv6 multicast pim-passive-enable**command to configure IPv6 PIM passive mode on a router. Once PIM passive mode is configured globally, use the **ipv6 pim passive** command in interface configuration mode to configure PIM passive mode on a specific interface.

Examples

The following example configures IPv6 PIM passive mode on a router:

```
Router(config)# ipv6 multicast pim-passive-enable
```

Related Commands

Command	Description
ipv6 pim passive	Configures PIM passive mode on a specific interface.

ipv6 multicast rpf

To enable IPv6 multicast reverse path forwarding (RPF) check to use Border Gateway Protocol (BGP) unicast routes in the Routing Information Base (RIB), use the **ipv6 multicast rpf**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 multicast [**vrf** *vrf-name*] **rpf backoff** *initial-delay max-delay* | **use-bgp**
no ipv6 multicast [**vrf** *vrf-name*] **rpf backoff** *initial-delay max-delay* | **use-bgp**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
backoff	Specifies the backoff delay after a unicast routing change.
initial-delay	Initial RPF backoff delay, in milliseconds (ms). The range is from 200 to 65535.
max-delay	Maximum RPF backoff delay, in ms. The range is from 200 to 65535.
use-bgp	Specifies to use BGP routes for multicast RPF lookups.

Command Default

The multicast RPF check does not use BGP unicast routes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI3	This command was integrated into Cisco IOS Release 12.2(33)SXI3.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **backoff** keyword and *initial-delay max-delay* arguments were added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

When the **ipv6 multicast rpf** command is configured, multicast RPF check uses BGP unicast routes in the RIB. This is not done by default.

Examples

The following example shows how to enable the multicast RPF check function:

```
Router# configure terminal
Router(config)# ipv6 multicast rpf use-bgp
```

Related Commands

Command	Description
ipv6 multicast limit	Configure per-interface multicast route (mroute) state limiters in IPv6.
ipv6 multicast multipath	Enables load splitting of IPv6 multicast traffic across multiple equal-cost paths.

ipv6 multicast rpf select

To configure Reverse Path Forwarding (RPF) lookups originating in a receiver Multicast VPN IPv6 (MVPNv6) routing and forwarding (MVRF) instance, to be performed in a source MVRF instance, based on group address, use the **ipv6 multicast rpf select** command in global configuration mode. To disable the functionality, use the **no** form of the command.

ip multicast vrf *receiver-vrf-name* **rpf select vrf** *source-vrf-name* **group-range** *access-list*
no ip multicast vrf *receiver-vrf-name* **rpf select vrf** *source-vrf-name* **group-range** *access-list*

Syntax Description

vrf *receiver-vrf-name*	Applies a group-based VRF selection policy to RPF lookups originating in the MVRF specified for the *receiver-vrf-name* argument.
vrf *source-vrf-name*	Specifies that the RPF lookups for groups matching the ACL specified with the **group-range** keyword and *access-list* argument be performed in the VRF specified for the *source-vrf-name* argument.
group-list *access-list*	Specifies the access control list (ACL) to be applied to the group-based VRF selection policy.

Command Default

No group-based VRF policy is configured.

Command Modes

Global configuration (config-term)

Command History

Release	Modification
15.3(1)S	This command was introduced.
Cisco IOS Xe 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **ipv6 multicast rpf select** command to configure group-based VRF selection policies.

This command uses the permit clauses of the specified ACL to define the set of ranges for which RPF selection will be done in the context of another VRF. Similarly, it uses the deny clauses of the ACL to define the set of ranges for which RPF selection will be done in the local context.

Note Deny and permit clauses of an ACL are not interpreted as an ordered set of rules on which to match groups. When you configure multiple instances of the **ipv6 multicast rpf select** command to apply RPF selection policies to different prefixes, on different VRFs, the result can include two or more RPF lookup configurations with overlapping permit ranges. For overlapping permit ranges, the system uses longest-prefix matching to select the RPF context. Consequently, a general deny statement at the beginning of an ACL is ignored for a more specific permit statement with a higher sequence number, and longer prefix, that appears later in the ACL.

Use the **show ipv6 rpf** command with the **select** keyword after configuring group-based VRF selection policies to display group-to-VRF mapping information.

Use the **show ipv6 rpf** command to display information for a VRF configuration.

Examples

The following example shows how to use a group-based VRF selection policy to configure the RPF lookup for groups that match ACL 1 to be performed in VPN-blue:

```
ipv6 multicast vrf VPN-red rpf select vrf VPN-blue group-range 1
!
.
.
.
!
access-list 1 permit ff02::00 00f0::00
!
```

Related Commands

Command	Description
show ipv6 rpf	Displays VRF configuration information.

ipv6 multicast-routing

To enable multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and to enable multicast forwarding, use the **ipv6 multicast-routing**command in global configuration mode. To stop multicast routing and forwarding, use the **no** form of this command.

ipv6 multicast-routing [**vrf** *vrf-name*]
no ipv6 multicast-routing

Syntax Description

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

Command Default

Multicast routing is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use the **ipv6 multicast-routing**command to enable multicast forwarding. This command also enables Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router being configured.

You can configure individual interfaces before you enable multicast so that you can then explicitly disable PIM and MLD protocol processing on those interfaces, as needed. Use the **no ipv6 pim** or the **no ipv6 mld router** command to disable IPv6 PIM or MLD router-side processing, respectively.

For the Cisco Catalyst 6500 and Cisco 7600 series routers, you must enable the **ipv6 multicast-routing** command to use IPv6 multicast routing. The **ipv6 multicast-routing** command need not be enbaled for IPv6 unicast-routing to function.

Examples

The following example enables multicast routing and turns on PIM and MLD on all interfaces:

```
ipv6 multicast-routing
```

Related Commands

Command	Description
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
no ipv6 pim	Turns off IPv6 PIM on a specified interface.
no ipv6 mld router	Disables MLD router-side processing on a specified interface.