ip mfib through ip multicast-routing

ip mfib

To reenable IPv4 multicast forwarding on the router, use the **ip mfib**command in global configuration mode. To disable IPv4 multicast forwarding, use the **no** form of this command.

ip mfib
no ip mfib

Syntax Description

This command has no arguments or keywords.

Command Default

IPv4 multicast forwarding is enabled automatically when IPv4 multicast routing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

After you have enabled the **ip multicast-routing** command, IPv4 multicast forwarding is enabled. Because IPv4 multicast forwarding is enabled by default, use the **no** form of the **ip mfib** command to disable IPv4 multicast forwarding.

Examples

The following example shows how to disable IPv4 multicast forwarding:

```
Router(config)# no ip mfib
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.

ip mfib cef

To reenable IPv4 Multicast Forwarding Information Base (MFIB) interrupt-level IP multicast forwarding of incoming packets or outgoing packets on a specific interface, use the **ip mfib cef input** command in interface configuration mode. To disable IPv4 MFIB interrupt-level IP multicast forwarding of incoming or outgoing packets on the interface, use the **no** form of this command.

ip mfib cef input | **output**
no ip mfib cef input | **output**

Syntax Description

input	Enables IPv4 MFIB interrupt-level IP multicast forwarding of incoming packets.
output	Enables IPv4 MFIB interrupt-level IP multicast forwarding of outgoing packets.

Command Default

Cisco Express Forwarding (CEF)-based (interrupt-level) forwarding of incoming packets and outgoing packets is enabled by default on interfaces that support it.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

After you have enabled the **ip multicast-routing** command, IPv4 MFIB interrupt-level switching of both incoming packets and outgoing packets is enabled by default on interfaces that support it.

Use the **no** form of the **ip mfib cef**command with the **input** keyword to disable IPv4 MFIB interrupt switching of incoming packets on a specific interface.

Use the **no** form of the **ip mfib cef**command with the **output** keyword to disable IPv4 MFIB interrupt switching of outgoing packets on a specific interface.

Use the **show ip mfib interface**command to display IPv4 MFIB-related information about interfaces and their forwarding status.

Examples

The following example shows how to disable MFIB interrupt-level IP multicast forwarding of incoming packets on Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib cef input
```

The following example shows how to disable MFIB interrupt-level IP multicast forwarding of outgoing packets on Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib cef output
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing
show ip mfib interface	Displays IPv4 MFIB-related information about interfaces and their forwarding status.

ip mfib forwarding

To reenable IPv4 multicast forwarding of packets received from or destined for the specified interface, use the **ip mfib forwarding**command in interface configuration mode. To disable multicast forwarding of multicast packets received from or destined for the specified interface, use the **no** form of this command.

ip mfib forwarding input | **output**
no ip mfib forwarding input | **output**

Syntax Description

input	Enables IPv4 multicast forwarding of packets received from an interface.
output	Enables IPv4 multicast forwarding of packets destined for an interface.

Command Default

IPv4 multicast forwarding is enabled automatically on all interfaces when IPv4 multicast routing is enabled.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	Support was not added for Cisco 7600 routers.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Because multicast forwarding is enabled automatically on all interfaces when IPv4 multicast routing is enabled using the **ip multicast-routing** command, the **ip mfib forwarding**command is used to reenable multicast forwarding of packets received from or destined for an interface, if it has been previously disabled.

Use the **no ip mfib forwarding**command with the **input** keyword to disable IPv4 multicast forwarding of packets received from an interface, although the specified interface will still continue to receive multicast packets destined for applications on the router itself.

Use the **no ip mfib forwarding** command with the **output** keyword to disable IPv4 multicast forwarding of packets destined for an interface.

Examples

The following example shows how to disable IPv4 multicast forwarding of packets received from Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib forwarding input
```

The following example shows how to disable IPv4 multicast forwarding of packets destined for Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib forwarding output
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.

ip mrm

To configure an interface to operate as a Test Sender or Test Receiver, or both, for Multicast Routing Monitor (MRM) tests, use the **ip mrm**command in interface configuration mode. To remove the interface as a Test Sender or Test Receiver, use the **no** form of this command.

ip mrm test-sender | **test-receiver** | **test-sender-receiver**
no ip mrm

Syntax Description

test-sender	Configures the interface to operate as a Test Sender.
test-receiver	Configures the interface to operate as a Test Receiver.
test-sender-receiver	Configures the interface to operate as both a Test Sender and Test Receiver (for different groups).

Command Default

No interface is configured to operate as a Test Sender or a Test Receiver, or both, for MRM.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(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

The Test Sender and Test Receiver can be either a router or a host.

If a router (or host) belongs to more than one test group, it can be a Test Sender for one group and a Test Receiver for the other group. It, however, cannot be the Test Sender and Test Receiver for the same group.

Examples

The following example shows how to configure an interface to operate as a Test Sender. In this example, Ethernet interface 0 is configured to operate as a Test Sender.

```
interface ethernet 0
 ip mrm test-sender
```

Related Commands

Command	Description
receivers	Establishes Test Receivers for MRM.
senders	Establishes Test Senders for MRM.

ip mrm accept-manager

To configure a Test Sender or Test Receiver to accept requests only from Managers that pass an access list, use the **ip mrm accept-manager**command in global configuration mode. To remove the restriction, use the **no** form of this command.

ip mrm accept-manager *access-list* [**test-sender** | **test-receiver**]
no ip mrm accept-manager *access-list*

Syntax Description

access-list	Number or name of an IP access list used to restrict Managers.
test-sender	(Optional) Applies the access list only to the Test Sender.
test-receiver	(Optional) Applies the access list only to the Test Receiver.

Command Default

Test Senders and Test Receivers respond to all Managers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(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

Use this command to control which Managers a Test Sender or Test Receiver must respond to.

If neither the **test-sender** nor **test-receiver** keyword is configured, the access list applies to both.

Examples

The following example shows how to configure a Test Sender to respond only to Managers that pass an access list. In this example, the Test Sender is configured to respond only to the Managers that pass the ACL named supervisor.

```
ip mrm accept-manager supervisor
!
ip access-list standard supervisor
 remark Permit only the Manager from the Central Office
 permit 172.18.2.4
!
```

Related Commands

Command	Description
ip mrm	Configures an interface to operate as a Test Sender or Test Receiver, or both, for MRM.

ip mrm manager

To specify the Multicast Routing Monitor (MRM) test to be created or modified and enter MRM manager configuration mode, use the **ip mrm manager**command in global configuration mode. To remove the test, use the **no** form of this command.

ip mrm manager *test-name*
no ip mrm manager *test-name*

Syntax Description

test-name	Name of the MRM test to be created or modified.

Command Default

No MRM tests are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(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

Use the **ip mrm manager** command to specify the name of the MRM test to be created or modified and enter MRM manager configuration mode where you specify the parameters of the MRM test.

Examples

The following example shows how to enter MRM manager configuration mode for the MRM test named test1:

```
Router(config)# ip mrm manager test1
Router(config-mrm-manager)#
```

Related Commands

Command	Description
mrm	Starts or stops an MRM test.
show ip mrm manager	Displays test information for MRM.

ip mroute

To configure a static multicast route (mroute), use the **ip mroute** command in global configuration mode. To remove the static mroute, use the **no** form of this command.

ip mroute [**vrf** *vrf-name*] *source-address mask* **fallback-lookupglobal** | **vrf** *vrf-name*[*protocol*]*rpf-address* | *interface-type interface-number*[*distance*]
no ip mroute [**vrf** *vrf-name*] *source-address mask* **fallback-lookupglobal** | **vrf** *vrf-name*[*protocol*][*distance*]

Cisco IOS Release 12.2(33)SRB and Subsequent 12.2SR Releases
ip mroute [**vrf** *vrf-name*] *source-address mask* **fallback-lookup global** | **vrf** *vrf-namerpf-address* | *interface-type interface-number* [*distance*]
no ip mroute [**vrf** *vrf-name*] *source-address mask*

Syntax Description

vrf *vrf-name*	(Optional) Configures a static mroute in the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
source-address	IP route prefix (A.B.C.D/n) or explicit IP address (A.B.C.D) of the source.
mask	Mask associated with the IP address or IP route prefix.
fallback-lookup {**global** | **vrf** *vrf-name*}	Specifies that the Reverse Path Forwarding (RPF) lookup originating in the receiver MVRF instance to continue and be resolved in either the global table or in the source MVRF instance. If you specify the **fallback-lookup** keyword, you must specify one of the following keywords and arguments: • **global** --Specifies that the source MVRF is in the global table. • **vrf** *vrf-name* --Specifies a VRF as the source MVRF.
protocol	(Optional) Unicast routing protocol or route map used to further tune the matching of source addresses.
rpf-address	IP address to be used as the RPF address. The interface associated with this IP address, thus, is used as the incoming interface for the mroute.
interface-type interface-number	Interface type and number to be used as the RPF interface for the mroute. A space is not needed between the values.
distance	(Optional) Administrative distance for the mroute. The value specified determines whether a unicast route, a Distance Vector Multicast Routing Protocol (DVMRP) route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the same distance as the other RPF sources, the static mroute will take precedence. The range is from 0 to 255. The default is 0.

Command Default

No static mroutes are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.0	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB	This command was modified. The **fallback-lookup** and **global**keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
12.2(33)SRB	This command was modified. The following protocol keywords were removed: **bgp**, **eigrp**, **isis**, **iso-igrp**, **mobile**, **odr**, **ospf**, **rip**, **route-map**, and **static**.
12.2(33)SXH	This command was modified. The **fallback-lookup** and **global**keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
12.2(33)SRC	This command was modified. The **fallback-lookup** and **global**keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
15.0(1)M	This command was modified. The **fallback-lookup** and **global**keywords and the **vrf**keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The **ip mroute** command is used to configure static mroutes. Static mroutes are similar to unicast static routes but differ in the following ways:

- Static mroutes are used to calculate RPF information, not to forward traffic.
- Static mroutes cannot be redistributed.

Static mroutes are strictly local to the router on which they are defined. Because Protocol Indepedent Multicast (PIM) does not have its own routing protocol, there is no mechanism to distribute static mroutes throughout the network. Consequently, the administration of static mroutes tends to be more complicated then the administration of unicast static routes.

When static mroutes are configured, they are stored on the router in a separate table referred to as the *static mroute table* . When configured, the **ip mroute** command enters a static mroute into the static mroute table for the source address or source address range specified for the *source-address* and *mask* arguments. Sources that match the source address or that fall in the source address range specified for the *source-address* argument will RPF to either the interface associated with the IP address specified for the *rpf-address* argument or the local interface on the router specified for the *interface-type* and *interface-number*arguments. If an IP address is specified for the *rpf-address*argument, a recursive lookup is done from the unicast routing table on this address to find the directly connected neighbor.

If there are multiple static mroutes configured, the router performs a longest-match lookup of the mroute table. When the mroute with the longest match (of the source-address) is found, the search terminates and the information in the matching static mroute is used. The order in which the static mroutes are configured is not important.

The administrative distance of an mroute may be specified for the optional *distance* argument. If a value is not specified for the *distance* argument, the distance of the mroute defaults to zero. If the static mroute has the same distance as another RPF source, the static mroute will take precedence. There are only two exceptions to this rule: directly connected routes and the default unicast route.

Tip Remember that the distance of a matching mroute is compared to the distance of any other matching routes found in the other sources of RPF information. The static mroute is used if its distance is equal to or less than the distance of other routes.

For the Multicast VPN Extranet Support feature, the **fallback-lookup** and **global**keywords and an additional **vrf** keyword and *vrf-name* argument were added to the syntax of the **ip mroute** command. Use the **ip mroute** command with the **fallback-lookup** keyword and **vrf** *vrf-name* keyword and argument to specify the source MVRF. By default, extranet MVPN relies on the unicast routing policies to determine the RPF interface. When the RPF lookup originates in a receiver MVRF, and it finds that the RPF interface is not located in the same MVRF, the router uses the information in the Border Gateway Protocol (BGP) imported route to determine the source MVRF. The RPF lookup then continues and resolves in the source MVRF. In cases where the multicast and unicast topologies are incongruent, you can override the default behavior by configuring a static mroute in the receiver MVRF to explicitly specify the source MVRF using the **ip mroute** command with the **fallback-lookup** keyword and **vrf** *vrf-name* keyword and argument.

Static mroutes can also be configured to support RPF for extranet MVPN in the case where the source is present in an MVRF and the receiver is in the global table. In this case, because BGP does not allow VPNv4 routes to be imported into the IPv4 routing table, unicast cannot obtain the source MVRF information needed to resolve the RPF lookup. To enable the RPF lookup to be resolved in this case, a static mroute can be configured to explicitly specify the source MVRF using the **ip mroute** command with the **fallback-lookup** keyword and the **global** keyword.

In Release 12.2(33)SRB and subsequent 12.2SR releases, the following protocol keywords are no longer supported (to be consistent with the **ip route** command): **bgp**, **eigrp**, **isis**, **iso-igrp**, **mobile**, **odr**, **ospf**, **rip**, **route-map**, and **static**. Those keywords are still present in the online help as available keywords; however, if the **ip mroute**command is entered with one of those deprecated protocol keywords, the command will be rejected and the following error message will display on the console: “The option of specifying protocol is deprecated.”

Examples

The following example shows how to configure a static mroute. In this static mroute configuration, the source IP address 10.1.1.1 is configured to be reachable through the interface associated with IP address 10.2.2.2:

```
ip mroute 10.1.1.1 255.255.255.255 10.2.2.2
```

The following example shows how to configure a static mroute. In this static mroute configuration, sources in network 172.16.0.0 are configured to be reachable through the interface associated with IP address 172.30.10.13:

```
ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
```

The following example shows how configure a static mroute. In this static mroute configuration (from an extranet MVPN configuration), RPF lookups originating in VPN-Y are configured to be resolved in VPN-X using the static mroute 192.168.1.1:

```
ip mroute vrf VPN-Y 192.168.1.1 255.255.255.255 fallback-lookup vrf VPN-X
```

ip mroute-cache

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip mroute-cache**command is not available in Cisco IOS software.

To configure IP multicast fast switching or multicast distributed switching (MDS), use the **ip mroute-cache** command in interface configuration mode. To disable either of these features, use the **no** form of this command.

ip mroute-cache [**distributed**]
no ip mroute-cache [**distributed**]

Syntax Description

distributed	(Optional) Enables MDS on the interface. In the case of Cisco 7500 series routers, this keyword is optional; if it is omitted, fast switching occurs. On the Cisco 12000 series, this keyword is required because the Cisco 12000 series does only distributed switching.

Command Default

On the Cisco 7500 series, IP multicast fast switching is enabled; MDS is disabled. On the Cisco 12000 series , MDS is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

On the Cisco 7500 Series

If multicast fast switching is disabled on an incoming interface for a multicast routing table entry, the packet will be sent at the process level for all interfaces in the outgoing interface list.

If multicast fast switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.

When multicast fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

If MDS is not enabled on an incoming interface that is capable of MDS, incoming multicast packets will not be distributed switched; they will be fast switched at the Route Processor (RP). Also, if the incoming interface is not capable of MDS, packets will get fast switched or process switched at the RP.

If MDS is enabled on the incoming interface, but at least one of the outgoing interfaces cannot fast switch, packets will be process switched. We recommend that you disable fast switching on any interface when MDS is enabled.

On the Cisco 12000 Series

On the Cisco 12000 series router, all interfaces should be configured for MDS because that is the only switching mode.

Examples

The following example shows how to enable IP multicast fast switching on the interface:

```
ip mroute-cache
```

The following example shows how to disable IP multicast fast switching on the interface:

```
no ip mroute-cache
```

The following example shows how to enable MDS on the interface:

```
ip mroute-cache distributed
```

The following example shows how to disable MDS and IP multicast fast switching on the interface:

```
no ip mroute-cache distributed
```

ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the **ip msdp border**command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*
no ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
sa-address	Specifies the active source IP address.
interface-type interface-number	Interface type and number from which the IP address is derived and used as the rendezvous point (RP) address in Source-Active (SA) messages. Thus, MSDP peers can forward SA messages away from this border. The IP address of the interface is used as the originator ID, which is the RP field in the MSDP SA message. No space is needed between the values.

Command Default

The active sources in the dense mode region will not participate in MSDP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command if you want the router to send SA messages for sources active in the PIM dense mode region to MSDP peers.

Specifying the interface-type and interface-number values allow the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.

Note We recommend configuring the border router in the sparse mode domain to proxy-register sources in the dense mode domain, and have the sparse mode domain use standard MSDP procedures to advertise these sources.

Note If you use this command, you must constrain the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in (S, G) state remaining long after a source in the dense mode domain has stopped sending.

Note The **ip msdp originator-id**command also identifies an interface type and number to be used as the RP address. If both the **ip msdp border**and **ip msdp originator-id**commands are configured, the address derived from the **ip msdp originator-id**command determines the address of the RP.

Examples

In the following example, the local router is not an RP. It borders a PIM sparse mode region with a dense mode region. It uses the IP address of Ethernet interface 0 as the "RP" address in SA messages.

```
ip msdp border sa-address ethernet0
```

Related Commands

Command	Description
ip msdp originator-id	Allows an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.
ip msdp redistribute	Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.

ip msdp cache-rejected-sa

To cache Source-Active (SA) request messages rejected from Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp cache-rejected-sa**command in global configuration mode. To stop tracking SA request messages, use the **no** form of this command.

ip msdp cache-rejected-sa *number-of-entries*
no ip msdp cache-rejected-sa *number-of-entries*

Syntax Description

number-of-entries	Number of entries to be cached. The range is from 1 to 32766.

Command Default

Rejected SA request messages are not stored.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.1E	This command was integrated into Cisco IOS Release 12.1E.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the ip msdp cache-rejected-sa command to configure the router to store SA messages that have been recently received from an MSDP peer but were rejected. Once this command is enabled, the router will maintain a rejected SAcache that stores the most recent rejected SA messages. The number of rejected SA message entries to be stored in the rejected SA cache is configured with the *number-of-entries* argument. If the rejected SA cache overflows, entries are overwritten, starting from the first entry.

Note Enabling the **ip msdp cache-rejected-sa** command will not impact the performance of MSDP.

Use the **show ip msdp sa-cache** command with the **rejected-sa** keyword to display SA messages rejected from MSDP peers.

Examples

The following example shows how to enable the router to store a maximum of 200 messages rejected from MSDP peers:

```
Router(config)# ip msdp cache-rejected-sa 200
```

Related Commands

Command	Description
show ip msdp sa-cache	Displays the (S, G) state learned from MSDP peers.

ip msdp cache-sa-state

To have the router create Source-Active (SA) state, use the **ip msdp cache-sa-state**command in global configuration mode.

ip msdp cache-sa-state [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Default

The router creates SA state for all Multicast Source Discovery Protocol (MSDP) SA messages it receives.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified such that it is enabled by default and cannot be disabled.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for 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 automatically configured if at least one MSDP peer is configured. It cannot be disabled.

If you are running a version of Cisco IOS software prior to Release 12.1(7), we recommend enabling the **ip msdp cache-sa-state** command.

Examples

The following example shows how the **ip msdp cache-sa-state** command is enabled when an MSDP peer is configured:

```
.
.
.
ip classless
ip msdp peer 192.168.1.2 connect-source Loopback0
ip msdp peer 192.169.1.7
ip msdp mesh-group outside-test 192.168.1.2
ip msdp cache-sa-state
ip msdp originator-id Loopback0
```

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP SA cache entries.
ip msdp sa-request	Configures the router to send SA request messages to the MSDP peer when a new joiner from the group becomes active.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

ip msdp default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **ip msdp default-peer**command in global configuration mode. To remove the default peer, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*]**default-peer***peer-addresspeer-name*[**prefix-list** *list*]
no ip msdp [**vrf** *vrf-name*] **default-peer**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address peer-name	IP address or Domain Name System (DNS) name of the MSDP default peer.
prefix-list *list*	(Optional) Specifies the Border Gateway Protocol (BGP) prefix list that specifies that the peer will be a default peer only for the prefixes listed in the list specified by the *list* argument. A BGP prefix list must be configured for this **prefix-list** *list* keyword and argument to have any effect.

Command Default

No default MSDP peer exists.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip msdp default-peer**command if you do not want to configure your MSDP peer to be a BGP peer also.

If only one MSDP peer is configured (with the **ip msdp peer** command), it will be used as a default peer. Therefore, you need not configure a default peer with this command.

If the **prefix-list** *list* keyword and argument are not specified, all SA messages received from the configured default peer are accepted.

Remember to configure a BGP prefix list if you intend to configure the **prefix-list** *list* keyword and argument with the **ip msdp default-peer**command.

If the **prefix-list** *list* keyword and argument are specified, SA messages originated from rendezvous points (RPs) specified by the **prefix-list** *list* keyword and argument will be accepted from the configured default peer. If the **prefix-list** *list* keyword and argument are specified but no prefix list is configured, the default peer will be used for all prefixes.

You can enter multiple **ip msdp default-peer**commands, with or without the **prefix-list** keyword, as follows. However, all commands must either have the keyword or all must not have the keyword.

- When you use multiple **ip msdp default-peer**commands with the **prefix-list** keyword, all the default peers are used at the same time for different RP prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.
- When you use multiple **ip msdp default-peer**commands without the **prefix-list** keyword, a single active peer is used to accept all SA messages. If that peer goes down, then the next configured default peer accepts all SA messages. This syntax is typically used at a stub site.

Examples

The following example shows how to configure the router at IP address 192.168.1.3 as the default peer to the local router:

```
ip msdp peer 192.168.1.3
ip msdp peer 192.168.3.5
ip msdp default-peer 192.168.1.3
```

The following example shows how to configure two default peers:

```
ip msdp peer 172.18.2.3
ip msdp peer 172.19.3.5
ip msdp default-peer 172.18.2.3 prefix-list site-c
ip prefix-list site-a permit 172.18.0.0/16
ip msdp default-peer 172.19.3.5 prefix-list site-a
ip prefix-list site-c permit 172.19.0.0/16
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip prefix-list	Creates a prefix list.

ip msdp description

To add descriptive text to the configuration for a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp description**command in global configuration mode. To remove the description, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **description** *peer-namepeer-address text*
no ip msdp [**vrf** *vrf-name*] **description** *peer-namepeer-address*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name peer-address	Peer name or address to which this description applies.
text	Description of the MSDP peer.

Command Default

No description is associated with an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Configure a description to make the MSDP peer easier to identify. This description is displayed in the output of the **show ip msdp peer** command.

Examples

The following example shows how to configure the router at the IP address 172.17.1.2 with a description indicating it is a router at customer A:

```
ip msdp description 172.17.1.2 router at customer a
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about the MSDP peer.

ip msdp filter-sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request**command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **filter-sa-request** *peer-addresspeer-name* [**list** *access-list*]
no ip msdp [**vrf** *vrf-name*] **filter-sa-request** *peer-addresspeer-name*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.
list *access-list*	(Optional) Specifies the standard IP access list number or name that describes a multicast group address. If no access list is specified, all SA request messages are ignored.

Command Default

By default, the router honors all SA request messages from peers. If this command is not configured, all SA request messages are honored. If this command is configured but no access list is specified, all SA request messages are ignored.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, the router honors all SA request messages from peers. Use this command if you want to control exactly which SA request messages the router will honor.

If no access list is specified, all SA request messages are ignored. If an access list is specified, only SA request messages from those groups permitted will be honored, and all others will be ignored.

Examples

The following example shows how to configure the router to filter SA request messages from the MSDP peer at 172.16.2.2. SA request messages from sources on the network 192.168.22.0 pass access list 1 and will be honored; all others will be ignored.

```
ip msdp filter-sa-request 172.16.2.2 list 1
access-list 1 permit 192.4.22.0 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp keepalive

To adjust the interval at which a Multicast Source Discovery Protocol (MSDP) peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down, use the **ip msdp keepalive** command in global configuration mode. To restore the default values, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **keepalive** *peer-addresspeer-name keepalive-interval hold-time-interval*
no ip msdp [**vrf** *vrf-name*] **keepalive** *peer-addresspeer-name*

Syntax Description

vrf *vrf-name*	(Optional) Configures the keepalive and hold-time intervals for the MSDP peer associated with the multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer whose keepalive timer and hold-time timer is to be adjusted.
keepalive-interval	Interval, in seconds, at which the MSDP peer will send keepalive messages. The range is from 1 to 60 seconds. The default is 60 seconds.
hold-time-interval	Interval, in seconds, at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. The range is from 1 to 75 seconds. The default is 75 seconds.

Command Default

An MSDP peer sends keepalives messages at an interval of once every 60 seconds. The hold-time interval for an MSDP peer is set to 75 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E4	This command was introduced.
12.2(5)	This command was integrated into Cisco IOS Release 12.2(5).
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip msdp keepalive** command to adjust the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.

Once an MSDP peering session is established, each side of the connection sends a keepalive message and sets a keepalive timer. If the keepalive timer expires, the local MSDP peer sends a keepalive message and restarts its keepalive timer; this interval is referred to as the keepalive interval. Use the *keepalive-interval*argument to adjust the interval for which keepalive messages will be sent. The keepalive

timer is set to the value specified for the *keepalive-interval*argument when the peer comes up. The keepalive timer is reset to the value of the *keepalive-interval* argument whenever an MSDP keepalive message is sent to the peer and reset when the timer expires. The keepalive timer is deleted when an MSDP peering session is closed. By default, the keepalive timer is set to 60 seconds.

Note The value specified for the *keepalive-interval* argument must be less than the value specified for the *holdtime-interval*argument and must be at least one second.

The hold-time timer is initialized to the value of the *hold-time-interval* argument whenever an MSDP peering connection is established, and is reset to value of the *hold-time-interval*argument whenever an MSDP keepalive message is received. The hold-time timer is deleted whenever an MSDP peering connection is closed. By default, the hold-time interval is set to 75 seconds.

Use the *hold-time-interval* argument to adjust the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. By default, it may take as long as 75 seconds for an MSDP peer to detect that a peering session with another MSDP peer has gone down. In network environments with redundant MSDP peers, decreasing the hold-time interval (by lowering the value for *hold-time-interval* argument from the default of 75 seconds) can expedite the reconvergence time of MSDP peers in the event that an MSDP peer fails.

Note It is recommended that you do not change the command defaults for the **ip msdp keepalive** command, as the command defaults are in accordance with RFC 3618, *Multicast Source Discovery Protocol* . If your network environment requires that you modify the defaults, you must configure the same time values for the *keepalive-interval* and *hold-time-interval* arguments on both ends of the MSDP peering session.

Examples

The following example shows how to set the keepalive interval to 40 seconds and the hold-time interval to 55 seconds for the MSDP peer at 172.16.100.10:

```
ip msdp keepalive 172.16.100.10 40 55
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp mesh-group

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **ip msdp mesh-group**command in global configuration mode. To remove an MSDP peer from a mesh group, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name peer-addresspeer-name*
no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name peer-addresspeer-name*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mesh-name	Name of the mesh group.
peer-address | *peer-name*	IP address or name of the MSDP peer to be a member of the mesh group.

Command Default

The MSDP peers do not belong to a mesh group.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. Source-Active (SA) messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group.

Mesh groups can be used to achieve two goals:

- To reduce SA message flooding
- To simplify peer-Reverse Path Forwarding (RPF) flooding (no need to run Border Gateway Protocol [BGP] or multiprotocol BGP among MSDP peers)

Examples

The following example shows how to configure the MSDP peer at address 192.168.1.3 to be a member of the mesh group named internal:

```
ip msdp mesh-group internal 192.168.1.3
```

ip msdp originator-id

To allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of the interface as the rendezvous point (RP) address in the SA message, use the **ip msdp originator-id**command in global configuration mode. To prevent the RP address from being derived in this way, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*
no ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and number on the local router whose IP address is used as the RP address in SA messages. No space is needed between the values.

Command Default

The RP address is used as the originator ID.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip msdp originator-id** command identifies an interface type and number to be used as the RP address in an SA message.

Use this command if you want to configure a logical RP. Because only RPs and MSDP border routers originate SAs, there are times when it is necessary to change the ID used for this purpose.

If both the **ip msdp border sa-address** and **ip msdp originator-id**commands are configured the address derived from the **ip msdp originator-id** command determines the address of the RP to be used in the SA message.

Examples

The following example shows how to configure the IP address of Ethernet interface 1 as the RP address in SA messages:

```
ip msdp originator-id ethernet1
```

Related Commands

Command	Description
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.

ip msdp password peer

To enable message digest 5 (MD5) password authentication for TCP connections between two Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp password peer** command in global configuration mode. To disable this function, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **password peer** *peer-namepeer-address* [*encryption-type*] *string*
no ip msdp [**vrf** *vrf-name*] **password peer** *peer-namepeer-address* [*encryption-type*] *string*

Syntax Description

vrf *vrf-name*	(Optional) Enables MD5 password authentication for TCP connections between MSDP peers associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
{*peer-name* | *peer-address*}	The Domain Name System (DNS) name or IP address of the MSDP peer for which to enable MD5 password authentication.
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Possible values are as follows: • **0** --Specifies that the text immediately following is not encrypted. • **7** --Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
string	Case-sensitive or encrypted password.

Command Default

MD5 password authentication for TCP connections between MSDP peers is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **ip msdp password peer** command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and verify the MD5 digest of every segment sent on the TCP connection.

If a router has a password configured for an MSDP peer, but the MSDP peer does not, a message such as the following will appear on the console while the routers attempt to establish a MSDP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

Configuring an MD5 Password in an Established MSDP Session

If you configure or change the password or key used for MD5 authentication between two MSDP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the keepalive period expires. If the password is not entered or changed on the remote router before the keepalive period expires, the session will time out and the MSDP session will reset.

Examples

The following example shows how to configure an MD5 password for TCP connections to the MSDP peer at 10.3.32.152:

```
ip msdp password peer 10.3.32.152 0 test
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about MSDP peers.

ip msdp peer

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp peer** command in global configuration mode. To remove the peer relationship, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **peer** *peer-namepeer-address* [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]
no ip msdp [**vrf** *vrf-name*] **peer** *peer-namepeer-address*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name peer-address	Domain Name System (DNS) name or IP address of the router that is to be the MSDP peer.
connect-source *interface-type interface-number*	(Optional) Specifies the interface type and number whose primary address becomes the source IP address for the TCP connection. This interface is on the router being configured.
remote-as *as-number*	(Optional) Specifies the autonomous system number of the MSDP peer. This keyword and argument are used for display purposes only.

Command Default

No MSDP peer is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The router specified should also be configured as a BGP neighbor.

The *interface-type* is on the router being configured.

If you are also BGP peering with this MSDP peer, you should use the same IP address for MSDP as you do for BGP. However, you are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as

there is a BGP or MBGP path between the MSDP peers. If there is no path, you must configure the **ip msdp default-peer** command.

The **remote-as** *as-number*keyword and argument are used for display purposes only.

A peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it displays as the autonomous system number of the peer.

Examples

The following example shows how to configure the router at the IP address 192.168.1.2 as an MSDP peer to the local router. The neighbor belongs to autonomous system 109.

```
ip msdp peer 192.168.1.2 connect-source ethernet 0/0
router bgp 110
 network 192.168.0.0
 neighbor 192.168.1.2 remote-as 109
 neighbor 192.168.1.2 update-source ethernet 0/0
```

The following example shows how to configure the router at the IP address 192.168.1.3 as an MSDP peer to the local router:

```
ip msdp peer 192.168.1.3
```

The following example shows how to configure the router at the IP address 192.168.1.4 to be an MSDP peer in autonomous system 109. The primary address of Ethernet interface 0/0 is used as the source address for the TCP connection.

```
ip msdp peer 192.168.1.4 connect-source ethernet 0/0 remote-as 109
```

Related Commands

Command	Description
ip msdp default-peer	Defines a default peer from which to accept all MSDP SA messages.
neighbor remote-as	Adds an entry to the BGP neighbor table.

ip msdp redistribute

To configure a filter to restrict which registered sources are advertised in SA messages, use the **ip msdp redistribute**command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **redistribute** [**list** *access-list-name*] [**asn** *as-access-list-number*] [**route-map** *map-name*]
no ip msdp [**vrf** *vrf-name*] **redistribute**

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the SA origination filter be applied to sources associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance.
list *access-list-name*	(Optional) Specifies that the router originate SA messages for local sources that are sending traffic to specific groups that match the (S, G) pairs defined in the extended access list.
asn *as-access-list-number*	(Optional) Specifies that the router originates SA messages that match the AS paths defined in the AS-path access list (configured using the **ip as-path** command). The AS-path access list number range is from 1 to 500. **Note** You can also specify a value of 0 after the **asn** keyword. If **asn 0** is specified, sources from all autonomous systems are advertised. This advertisement capability is useful when you are connecting a Protocol Independent Multicast (PIM) dense mode (PIM-DM) domain to a PIM sparse mode (PIM-SM) domain running MSDP or when you have configured MSDP on a router that is not configured with Border Gateway Protocol (BGP).
route-map *map-name*	(Optional) Specifies that the router originate SA messages for local sources that match the criteria defined in a route map.

Command Default

- If this command is not configured in a multicast network using MSDP to interconnect PIM-SM domains, only local sources are advertised in SA messages, provided the local sources are sending to groups for which the router is a rendezvous point (RP).
- If this command is not configured and if the **ip msdp border sa-address** command is configured, all local sources are advertised.
- If the **ip msdp redistribute** command is configured with no keywords and arguments, no multicast sources are advertised in SA messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, an RP that is configured to run MSDP will originate SA messages for all local sources for which it is the RP. Local sources that register with an RP, therefore, will be advertised in SA messages, which in some cases is not desirable.

To control what sources are advertised in SA messages, you can configure SA origination filters on an RP using the **ip msdp redistribute** command. By creating SA origination filters, you can control the sources advertised in SA messages as follows:

- You can prevent an RP from originating SA messages for local sources by configuring the **ip msdp redistribute** command without any keywords or arguments. Issuing this form of the command effectively prevents the router from advertising local sources in SA messages.

Note When the **ip msdp redistribute** command is entered without any keywords or arguments, the router will still forward SA messages from other MSDP peers in the normal fashion; it will just not originate any SA messages for local sources.

- You can configure the router to originate SA messages for (S, G) pairs defined in an extended access list by configuring the **ip msdp redistribute** command with the optional **list** keyword and *access-list-name* argument. Issuing this form of the command effectively configures the router to originate SA messages for local sources that are sending traffic to specific groups that match (S, G) pairs defined in the extended access list. All other local sources will not be advertised in SA messages.
- You can configure the router to originate SA messages for AS paths defined in an AS-path access list by configuring the **ip msdp redistribute** command with the optional **asn** keyword and *as-access-list-number*argument. Issuing this form of the command effectively configures the router to originate SA messages for local sources that are sending traffic to specific groups that the match AS paths defined in an AS-path access list. All other local sources will not be advertised in SA messages.

Note AS-path access lists are configured using the **ip as-path access-list** command.

- You can configure the router to originate SA messages for local sources that match the criteria defined in a route map by configuring the **ip msdp redistribute** command with the optional **route-map** keyword and *map-name* argument. Issuing this form of the command effectively configures the router to originate SA messages for local sources that match the criteria defined in the route map. All other local sources will not be advertised in SA messages.

Note You can configure an SA origination filter that includes an extended access list, an AS-path access list, and a route map (or a combination thereof). In that case, all conditions must be true before any local sources are advertised in SA messages.

Tip This command affects SA message origination, not SA message forwarding or receipt. If you want to control the forwarding of SA messages to MSDP peers or control the receipt of SA messages from MSDP peers, use the **ip msdp sa-filter out**command or the **ip msdp sa-filter in**command, respectively.

Examples

The following example shows how to configure which (S, G) entries from the mroute table are advertised in SA messages originated from AS 64512:

```
ip msdp redistribute route-map customer-sources
route-map customer-sources permit
match as-path 100
ip as-path access-list 100 permit ^64512$
```

Related Commands

Command	Description
ip as-path	Defines a BGP-related access list.
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for SA messages sent to the MSDP peer.

ip msdp rpf rfc3618

To enable Multicast Source Discovery Protocol (MSDP) peers to be compliant with peer-Reverse Path Forwarding (RPF) forwarding rules specified in Internet Engineering Task Force (IETF) RFC 3618, use the **ip msdp rpf rfc3618**command in global configuration mode. To revert MSDP peers to non-IETF compliant peer-RPF forwarding rules, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **rpf rfc3618**
no ip msdp [**vrf** *vrf-name*] **rpf rfc3618**

Syntax Description

vrf *vrf-name*	(Optional) Enables MSDP peers associated with the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance specified for the *vrf-name*argument to be compliant with the peer-RPF forwarding rules specified in RFC 3618.

Command Default

MSDP peers are not compliant with peer-RPF forwarding rules specified in RFC 3618.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to enable MSDP peers to be compliant with peer-RPF forwarding rules specified in RFC 3618. Such compliance allows you to use Border Gateway Protocol (BGP) route reflectors without running MSDP on them. It also allows you to use an Interior Gateway Protocol (IGP) for the RPF check and thereby run peerings without BGP or Multicast Border Gateway Protocol (MBGP).

Examples

The following example shows how to enable MSDP peer-RPF forwarding rules that are compliant with RFC 3618:

```
ip msdp rpf rfc3618
```

Related Commands

Command	Description
show ip msdp rpf-peer	Displays the unique MSDP peer information from which the router will accept SA messages originating from the specified RP.

ip msdp sa-filter in

To configure an incoming filter list for Source-Active (SA) messages received from the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter in**command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter in** *peer-addresspeer-name* [**list** *access-list-name*] [**route-map** *map-name*] [**rp-list** *access-list-rangeaccess-list-name*] [**rp-route-map** *route-map reference*]
no ip msdp [**vrf** *vrf-name*] **sa-filter in** *peer-addresspeer-name*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer to which the SA messages are filtered.
list *access-list-name*	(Optional) Specifies the IP access list to pass certain source and group pairs.
route-map *map-name*	(Optional) Specifies the route map match criteria for passing certain source and group pairs.
rp-list	(Optional) Specifies an access list for an originating Route Processor.
access-list-range	Number assigned to an access ist. The range is from 1 to 99.
access-list-name	Name assigned to an access list.
rp-route-map *route-map reference*	(Optional) Specifies the route map and route reference for passsing through a route processor.

Command Default

No incoming messages are filtered; all SA messages are accepted from the peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf**keyword and *vrf-name*argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was modified. Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **rp-list** keyword was added.

Usage Guidelines

If you use the **ip msdp sa-filter in**command without specifying access list name or route map match criteria, all source/group pairs from the peer are filtered.

If you use the **route-map** *map-name* keyword and argument pair, the specified MSDP peer passes only those SA messages that meet the match criteria.

If all match criteria are true, a **permit** keyword from the route map passes the routes through the filter. A **deny** keyword will filter routes.

Examples

The following example shows how to configure the router to filter all SA messages from the peer at 192.168.1.3:

```
Router> enable
Router# configure terminal
Router(config)# ip msdp peer 192.168.1.3 connect-source Ethernet 0/0
Router(config)# ip msdp sa-filter in 192.168.1.3
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for SA messages sent to the specified MSDP peer.

ip msdp sa-filter out

To configure an outgoing filter list for Source-Active (SA) messages sent to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter out**command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp[**vrf** *vrf-name*]**sa-filter out** *peer-addresspeer-name*[**list** *access-list-name*][**route-map** *map-name*][**rp-list***access-list-rangeaccess-list-name*][**rp-route-map** *route-map reference*]
no ip msdp[**vrf** *vrf-name*]**sa-filter out** *peer-addresspeer-name*

Syntax Description

vrf	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer to which the SA messages are filtered.
list *access-list-name*	(Optional) Specifies the IP access list to pass certain source and group pairs.
route-map *map-name*	(Optional) Specifies the route map match criteria for passing certain source and group pairs.
rp-list	(Optional) Specifies an access list for an originating Route Processor.
access-list range	Number assigned to an access list. The range is from 1 to 99.
access-list name	Name assigned to an access list.
rp-route-map *route-map reference*	(Optional) Specifies the route map and route reference for passsing through a route processor.

Command Default

No outgoing messages are filtered; all SA messages received are forwarded to the peer.

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was modified. Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **rp-list** keyword was added.

Usage Guidelines

If you use the **ip msdp sa-filter out** command without specifying access list name or route map match criteria, all source and group pairs from the peer are filtered. If you do specify an access-list name, the specified MSDP peer passes only those SA messages that pass the extended access list.

If you use the **route-map** *map-name* keyword and argument pair, the specified MSDP peer passes only those SA messages that meet the match criteria.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any source and group pairs in outgoing SA messages.

If all match criteria are true, a **permit** keyword from the route map will pass routes through the filter. A **deny** keyword will filter routes.

Examples

The following example shows how to permit only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer at the IP address 192.168.1.5:

```
Router> enable
Router# configure terminal
Router(config)# ip msdp peer 192.168.1.5 connect-source ethernet 0/0
Router(config)# ip msdp sa-filter out 192.168.1.5 list 100
Router(config)# access-list 100 permit ip 172.1.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.

ip msdp sa-limit

To limit the number of Source Active (SA) messages that can be added to the SA cache from a specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-limit** command in global configuration mode. To remove the limit imposed by the MSDP SA limiter, use the **no** form of this command.

ip msdp[**vrf** *vrf-name*]**sa-limit** *peer-addresspeer-name*[*sa-limit*]
no ip msdp[**vrf** *vrf-name*]**sa-limit** *peer-addresspeer-name*[*sa-limit*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the MSDP SA limiter be applied to the MSDP peer associated with Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-name peer-address	Domain Name System (DNS) name or IP address of the MSDP peer for which to apply the MSDP SA limiter.
sa-limit	Maximum number of SA messages that can be accepted (cached) from the specified peer. The range is from 1 to 2147483646.

Command Default

No MSDP SA limiters are configured for MSDP peers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(3)	This command was integrated into Cisco IOS Release 12.2(3).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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

Use this command to configure MSDP SA limiters, which impose limits on the number of MSDP SA messages that an MSDP-enabled router can accept (can be cached) from an MSDP peer. This command provides a means to protect an MSDP-enabled router from denial of service (DoS) attacks.

Mechanics of MSDP SA Limiters

- When MSDP SA limiters are configured, the router maintains a per-peer count of SA messages stored in the SA cache.
- SA messages that exceed the limit configured for an MSDP peer are ignored.
- If the router receives SA messages in excess of the configured limit from an MSDP peer, a warning in the following format is generated (once a minute) until the cache is cleared:

```
%MSDP-4-SA_LIMIT: SA from peer <peer address or name>, RP <RP address> for <mroute> exceeded
 sa-limit of <configured SA limit for MSDP peer>
```

Tips for Configuring MSDP SA Limiters

- We recommended that you configure MSDP SA limiters for all MSDP peerings on the router.
- An appropriately low MSDP SA limit should be configured on peerings with a stub MSDP region (an MSDP peer that may have some further downstream peers but does not act as a transit for SA messages across the rest of the Internet).
- An appropriately high SA limit should be configured for all MSDP peerings that act as transits for MSDP SA messages across the Internet.

The output of the **show ip msdp count**, **show ip msdp peer**, and **show ip msdp summary**commands will display the number of SA messages from each MSDP peer that is in the SA cache. If the **ip msdp sa-limit** command is configured, the output of the **show ip msdp peer** command will also display the value of the SA message limit for each MSDP peer.

Examples

The following example shows how to configure an MSDP SA limiter. In this example, an MSDP SA limiter is configured that imposes a limit of 100 SA messages from the MSDP peer at 192.168.10.1.

```
ip msdp sa-limit 192.168.10.1 100
```

Related Commands

Command	Description
show ip msdp count	Displays the number of sources and groups originated in MSDP SA messages.
show ip msdp peer	Displays detailed information about the MSDP peer.
show ip msdp summary	Displays MSDP peer status.

ip msdp sa-request

Note Effective with Cisco IOS Release 12.0(27)S, 12.2(20)S, 12.2(18)SXE, and 12.3(4)T, the **ip msdp sa-request** is not available in Cisco IOS software.

To configure the router to send Source-Active (SA) request messages to an Multicast Source Discovery Protocol (MSDP) peer when a new joiner from the group becomes active, use the **ip msdp sa-request**command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-request** *peer-addresspeer-name*
no ip msdp [**vrf** *vrf-name*] **sa-request** *peer-addresspeer-name*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.

Command Default

The router does not send SA request messages to the MSDP peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.0(27)S	This command was removed from Cisco IOS Release 12.0(27)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S	This command was removed from Cisco IOS Release 12.2(20)S.
12.2(18)SXE	This command was removed from Cisco IOS Release 12.2(18)SXE.
12.3(4)T	This command was removed from Cisco IOS Release 12.3(4)T.

Usage Guidelines

By default, the router does not send any SA request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive any SA messages that eventually arrive.

Use this command if you want a new member of a group to learn the current, active multicast sources in a connected Protocol Independent Multicast sparse mode (PIM-SM) domain that are sending to a group. The router will send SA request messages to the specified MSDP peer when a new member joins a group. The

peer replies with the information in its SA cache. If the peer does not have a cache configured, this command provides nothing.

An alternative to this command is using the **ip msdp cache-sa-state** command to have the router cache messages.

Examples

The following example shows how to configure the router to send SA request messages to the MSDP peer at the IP address 192.168.10.1:

```
ip msdp sa-request 192.168.10.1
```

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.
ip msdp peer	Configures an MSDP peer.

ip msdp shutdown

To administratively shut down a configured Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp shutdown**command in global configuration mode. To bring the peer back up, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **shutdown** *peer-addresspeer-name*
no ip msdp [**vrf** *vrf-name*] **shutdown** *peer-addresspeer-name*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to shut down.

Command Default

No action is taken to shut down an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to shut down the MSDP peer at IP address 192.168.7.20:

```
ip msdp shutdown 192.168.7.20
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp timer

To adjust the interval at which Multicast Source Discovery Protocol (MSDP) peers will wait after peering sessions are reset before attempting to reestablish the peering sessions, use the **ip msdp timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **timer** *connection-retry-interval*
no ip msdp [**vrf** *vrf-name*] **timer**

Syntax Description

vrf *vrf-name*	(Optional) Sets the connection-retry interval for MSDP peers associated with the multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
connection-retry-interval	Interval, in seconds, at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. The range is from 1 to 60 seconds. The default is 30 seconds.

Command Default

An MSDP peer will wait 30 seconds after a peering session is reset before attempting to reestablish the peering session with any peer.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E4	This command was introduced.
12.2(5)	This command was integrated into Cisco IOS Release 12.2(5).
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip msdp timer** command to adjust the interval at which all MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. This interval is referred to as the connection-retry interval. By default, MSDP peers will wait 30 seconds after is session is reset before attempting to reestablish sessions with other peers. When the **ip msdp timer** command is configured, the configured connection-retry interval applies to all MSDP peering sessions on the router.

In network environments where fast recovery of Source-Active (SA) messages is required (such as in trading floor network environments), you may want to decrease the connection-retry interval to a time value less than the default value of 30 seconds.

Examples

The following example shows how to set the connection-retry interval for all MSDP peers to 20 seconds:

```
ip msdp timer 20
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp ttl-threshold

To limit which multicast data packets are sent in Source-Active (SA) messages to a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp ttl-threshold**command in global configuration mode. To restore the default value, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **ttl-threshold** *peer-addresspeer-name ttl-value*
no ip msdp [**vrf** *vrf-name*] **ttl-threshold** *peer-addresspeer-name*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the *ttl-value* argument value applies.
ttl-value	Time-to-live (TTL) value; valid values are from 0 to 255. The default value of the *ttl-value* argument is 0, meaning all multicast data packets are forwarded to the peer until the TTL is exhausted.

Command Default

ttl-value : 0

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command limits which multicast data packets are sent in data-encapsulated SA messages. Only multicast packets with an IP header TTL greater than or equal to the *ttl-value* argument are sent to the MSDP peer specified by the IP address or name.

Use this command if you want to use TTL to scope your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you would need to send those packets with a TTL greater than 8.

The default value of the *ttl-value* argument is 0, which means that all multicast data packets are forwarded to the peer until the TTL is exhausted.

Examples

The following example shows how to configure a TTL threshold of 8 hops:

```
ip msdp ttl-threshold 192.168.1.5 8
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip multicast boundary

To configure an IPv4 multicast boundary on an interface for a specified scope, use the **ip multicast boundary** command in interface configuration mode and virtual network interface . To remove the boundary, use the **no** form of this command.

ip multicast boundary *access-list* [**filter-autorp**]
no ip multicast boundary *access-list* [**filter-autorp**]

Cisco IOS Release 12.3(11)T and Subsequent T and Mainline Releases
ip multicast boundary *access-list* [**filter-autorp** | **in** | **out**]
no ip multicast boundary *access-list* [**filter-autorp** | **in** | **out**]

Cisco IOS XE Release 3.13S and Later Releases
ip multicast boundary block source
no ip multicast boundary block source

Syntax Description

access-list	Number or name that identifies an access control list (ACL) that controls the range of group addresses or (S, G) traffic affected by the boundary.
block source	Blocks the source of all incoming multicast traffic on an interface.
filter-autorp	(Optional) Filters auto-rendezvous point (Auto-RP) messages denied by the boundary ACL.
in	(Optional) Filters source traffic coming into the interface that is denied by the boundary ACL.
out	(Optional) Prevents multicast route (mroute) states from being created on an interface by filtering Protocol Independent Multicast (PIM) joins and Internet Group Management Protocol (IGMP) reports for groups or channels that are denied by the boundary ACL.

Command Default

No user-defined boundaries are configured.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS 11.1	This command was introduced.
Cisco IOS 12.0(22)S	This command was modified. The **filter-autorp** keyword was added.
Cisco IOS 12.1(12c)E	This command was modified. The **filter-autorp** keyword was integrated into Cisco IOS Release 12.1(12c)E.
Cisco IOS 12.2(11)	This command was modified. The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(11).
Cisco IOS 12.2(13)T	This command was modified. The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(13)T.

Release	Modification
Cisco IOS 12.3(11)T	This command was modified. The **in** and **out** keywords were added.
Cisco IOS 12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS 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.
Cisco IOS XE 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode. The *access-list* argument and **filter-autorp** keyword are no longer required with the **no** form of this command to remove the boundary ACL configuration.
Cisco IOS XE 3.13S	This command was modified. The **block** and **source** keywords were added.

Usage Guidelines

Use the **ip multicast boundary** command to configure an administratively scoped (user-defined) boundary on an interface in order to filter source traffic coming into the interface and prevent mroute states from being created on the interface.

Note An IP multicast boundary enables reuse of the same multicast group address in different administrative domains.

A standard ACL is used with the **ip multicast boundary** command to define the group address range to be permitted or denied on an interface. An extended ACL is used with the **ip multicast boundary** to define (S, G) traffic to be permitted or denied on an interface. Extended ACLs can also be used to define the (*, G) state to be permitted or denied on an interface, by specifying **host 0.0.0.0** for the source address in the permit statements that compose the extended ACL.

When you configure IP multicast boundaries for (S, G) traffic in an Any Source Multicast (ASM) network environment-to ensure that the IP multicast boundaries function properly-you must configure an extended ACL on routers along the rendezvous point tree (RPT) that permits:

- (S, G) traffic by specifying the source and group address range in permit statements.
- (*, G) traffic by specifying **host 0.0.0.0** for the source address followed by the group address or group address range in permit statements.
- Traffic destined to the rendezvous point (RP) by including permit statements for (RP, G), where the IP address of the RP is specified for the source followed by the group address or group address range.

The IP multicast boundary guideline for ASM applies only to the routers on the RPT from the last-hop router to the RP. For routers on the RP-to-source branch, you need to define only the (S, G) traffic in the extended ACL (by specifying the source and group address range in permit statements).

When you configure IP multicast boundaries for (S, G) traffic in a Source Specific Multicast (SSM) network environment, you need to define only the (S, G) traffic to be permitted or denied on an interface in the extended ACL.

IP multicast boundaries filter data and control plane traffic including IGMP, PIM Join and Prune, and Auto-RP messages. The following messages are not filtered by IP multicast boundaries:

- PIM Register messages are sent using multicast and not filtered.
- PIM Hellos for neighbor-ship to 224.0.0.13 are not filtered.
- Link local messages are not affected and PIM hellos on the local segment are not filtered. To disallow PIM adjacency formation on each link, use the **ip pim neighbor-filter** command in the interface or virtual network interface configuration mode.

If you configure the **filter-autorp** keyword, the user-defined boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Note Extended ACLs cannot be used with the **filter-autorp** keyword because Auto-RP announcements do not contain source addresses.

In Cisco IOS software releases that do not support the **in** and **out** keywords, the IP multicast boundary both filters source traffic coming into the interface and prevents mroute states from being created on the interface.

In Cisco IOS releases that support the **in** and **out** keywords, these keywords are used as follows:

- The **in** keyword is used to filter source traffic coming into the interface.
- The **out** keyword is used to prevent mroute states from being created on an interface; that is, it will prevent IGMP reports and PIM joins from creating mroutes states for groups and channels denied by the boundary ACL, and the interface will not be included in the outgoing interface list (OIL).
- If a direction is not specified with the **ip multicast boundary** command, the IP multicast boundary both filters source traffic coming into the interface and prevents mroute states from being created on the interface.

In addition, the following rules govern the use of the **in**, **out**, and **filter-autorp** keywords with the **ip multicast boundary** command:

- The **in** and **out** keywords support standard or extended ACLs for (S, G) filtering.
- The **in** and **out** keywords support standard or extended ACLs for SSM filtering.
- One instance of the **in** and **out** keywords can be configured on an interface.
- Only standard ACLs are permitted with the use of the **filter-autorp** keyword.

In Cisco 7600 series routers:

- A deny any statement at the end of the boundary ACL will cause all multicast boundaries including the link local address in the range (224.0.0.0 - 224.0.0.255) to be dropped in the hardware.
- When the ip multicast boundary *access-list* [**filter-autorp**] command is configured with an empty ACL, it interferes in the proper functioning of Auto-RP in the hardware. Hence, it is important to specify the address you want to allow or deny in the access-list.

In Cisco IOS XE Release 3.2S and later releases, the *access-list* and **filter-autorp** argument and keyword are no longer required with the **no** form of this command.

In Cisco IOS XE Release 3.1S and earlier releases, the **no ip multicast boundary** command must be configured with the ACL and the **filter-autorp** keyword to remove the boundary ACL configuration.

A maximum of three instances of an **ip multicast boundary** command is allowed on an interface: one instance of the command with the **in** keyword, one instance of the command with the **out** keyword, and one instance of the command with or without the **filter-autorp** keyword.

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

Examples

The following example shows how to set up an IP multicast boundary for all user-defined IPv4 multicast addresses by denying the entire user-defined IPv4 multicast address space (239.0.0.0/8). All other Class D addresses are permitted (224.0.0.0/4).

```
access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
interface ethernet 0
 ip multicast boundary 1
```

The following example shows how to set up an IP multicast boundary in an SSM network environment. In this example, the IP multicast boundary is configured to permit mroute states for (172.16.2.201, 232.1.1.1) and (172.16.2.202, 232.1.1.1). All other (S, G) traffic is implicitly denied.

```
ip access-list extended acc_grp1
permit ip host 172.16.2.201 host 232.1.1.1
permit ip host 172.16.2.202 host 232.1.1.1
interface ethernet 2/3
 ip multicast boundary acc_grp1 out
```

The following example shows how to configure an IP multicast boundary in an ASM network environment. In this example, the IP multicast boundary configuration on the last-hop router is shown. The topology for this example is not illustrated; however, assume that the IP address of the RP in this scenario is 10.1.255.104. The IP multicast boundary is configured to filter outgoing IP multicast traffic on Fast Ethernet interface 0/0. The boundary ACL used for the IP multicast boundary in this scenario contains three permit statements:

- The first permit statement specifies the (S, G) traffic to be permitted.
- The second permit statement specifies the (RP, G) traffic to be permitted.
- The third permit statement specifies the (*, G) traffic to be permitted.

All other outgoing multicast traffic on this interface is implicitly denied.

```
ip access-list extended bndry-asm-3
 permit ip host 10.1.248.120 239.255.0.0 0.0.255.255
 permit ip host 10.1.255.104 239.255.0.0 0.0.255.255
 permit ip host 0.0.0.0 239.255.0.0 0.0.255.255
interface FastEthernet0/0
 ip multicast boundary bndry-asm-3 out
```

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)# ip multicast boundary block source
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating PIM.

ip multicast cache-headers

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip multicast cache-headers** command is not available in Cisco IOS software.

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command in global configuration mode. To remove the buffer, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]
no ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]

Syntax Description

vrf *vrf-name*	(Optional) Allocates a circular buffer to store IP multicast packet headers associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rtp	(Optional) Caches Real-Time Transport Protocol (RTP) headers.

Command Default

The command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1	The **rtp** keyword was added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

IP multicast packet headers can be stored in a cache and then displayed to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay

- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- User Datagram Protocol (UDP) port numbers
- Packet length

Use the **show ip mpacket** command to display the buffer.

Examples

The following example shows how to allocate a buffer to store IP multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache header buffer.

ip multicast default-rpf-distance

When configuring Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), to change the distance given to the default Reverse Path Forwarding (RPF) interface, use the **ip multicast default-rpf-distance** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip multicast default-rpf-distance *distance*
no ip multicast default-rpf-distance *distance*

Syntax Description

distance	Distance given to the default RPF interface. The default value is 15.

Command Default

distance : 15

Command Modes

Global configuration

Command History

Release	Modification
12.0(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

This command is optional. If you want to receive all multicast traffic from all sources on the unidirectional link (UDL), as long as 15 is the lowest distance, you need not change the value of 15.

The default RPF interface is selected when an IGMP query message is received on a UDL and indicates to the router that all sources will use RPF to reach the UDL interface.

Any explicit sources learned by routing protocols will take preference as long as their distance is less than the *distance* argument configured with the **ip multicast default-rpf-distance** command.

You might consider changing the default value for one of the following reasons:

- To make IGMP prefer the UDL.
- To configure a value less than existing routing protocols.
- If you want to receive multicast packets from sources on interfaces other than the UDL interface. Configure a value greater than the distances of the existing routing protocols to make IGMP prefer the nonunidirectional link.

Examples

The following example configures a distance of 20:

```
ip multicast default-rpf-distance 20
```

Related Commands

Command	Description
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip multicast group-range

To define a global range of IP multicast groups and channels to be permitted or denied, use the **ip multicast group-range** command in global configuration mode. To remove the global IP multicast address group range, use the **no** form of this command.

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

Syntax Description

vrf *vrf-name*	(Optional) Applies the multicast group address range to group addresses associated with the Multicast Virtual Private Network (MVPN) routing and forwarding instance (MVRF) specified for the *vrf-name* argument.
access-list	Access control list (ACL) that defines the multicast groups to be permitted or denied.

Command Default

A global IP multicast group address range is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	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 integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(1)SG	This command was integrated into Cisco IOS Release15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **ip multicast group-range** command to define a global range of IP multicast groups and channels to be permitted or denied. This command is used to disable multicast protocol actions and traffic forwarding for unauthorized groups or channels for all interfaces on the router.

Use the optional **vrf** keyword with the *vrf-name* argument to apply an IP multicast group address range to the MVRF instance specified for the *vrf-name* argument.

For the required *access-list* argument, specify an access list that defines the multicast groups or channels to be permitted or denied globally:

- A standard ACL can be used to define the group address range to be permitted or denied globally.
- An extended ACL is used with the **ip multicast group-range** command to define (S, G) traffic to be permitted or denied globally. Extended ACLs can also be used to define the (*, G) state to be permitted or denied globally, by specifying **host 0.0.0.0** for the source address in the permit statements that compose the extended ACL.

Note When using the **ip multicast group-range** command to configure a multicast address group range in an AutoRP network, you must explicitly permit the AutoRP groups (39/40) in the access list that defines the range; if not, AutoRP packets will not be accepted or forwarded.

Note If AutoRP is enabled, but a specific group range is denied (for example, 224/8), an AutoRP message for that range will be accepted and the RP mapping will be put into the cache. However, state will not be created for those groups.

Examples

Allowing Groups 239/8 and AutoRP Groups (.39 and .40) to Operate in an Enterprise Network

The following example shows how to configure an IP multicast address group range that allows the 239/8 range and AutoRP groups to operate in an enterprise network:

```
ip multicast group-range 1
access-list 1 permit 224.0.1.39 0.0.0.0
access-list 1 permit 224.0.1.40 0.0.0.0
access-list 1 permit 239.0.0.0 0.255.255.255
```

Allowing Groups 239/8 in a Campus Network and Groups 239/9 on Interfaces Connected to Remote Branches

The following example shows how to configure an IP multicast group range that permits groups 239/8 in a campus network. For remote branches connected through Serial interface 0, an IP multicast boundary is configured to further refine the groups permitted to 239/9.

```
ip multicast group-range 1
access-list 1 permit 239.0.0.0 0.255.255.255
interface Serial 0
  ip multicast boundary 2
access-list 2 permit 239.128.0.0 0.127.255.255
```

Allowing Groups 239/8 Globally and AutoRP Groups (.39 and .40) on Core-Facing Interfaces

The following example shows how to configure an IP multicast group range that allows the 239/8 range. In this example, AutoRP groups are denied on access interfaces and permitted on core-facing interfaces. In addition, to permit AutoRP groups on core-facing interfaces, an IP multicast boundary is configured in this example that permits AutoRP groups (.39 and .40).

```
ip multicast group-range 1
access-list 1 permit 239.0.0.0 0.255.255.255
interface Ethernet 0
 description access interface
 ip pim sparse-mode
interface Ethernet 1
 description core facing interface
 ip multicast boundary 2
```

```
access-list 2 permit 224.0.1.39
access-list 2 permit 224.0.1.40
access-list 2 permit 239.0.0.0 0.255.255.255
```

ip multicast hardware-switching non-rpf aging

To configure the multicast hardware switching for rate-limiting of non-RP aging traffic, use the ip multicast hardware-switching non-rpf aging command in global configuration mode . To disable, use the **no** form of this command.

ip multicast hardware-switching non-rpf aging fast *2-10* | **global** *0-180*
no ip multicast hardware-switching non-rpf aging fast *2-10* | **global** *0-180*

Syntax Description

fast	Enables NON-RPF aging fast timer.
2-10	Fast aging timing interval.
global	Enables NON-RPF aging global timer.
0-180	Global aging time interval.

Command Default

The default state is OFF.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRE	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the multicast hardware switching for rate-limiting of non-RP traffic:

```
Router# enable
Router# configure terminal
Router(config)# ip multicast hardware-switching non-rp aging
```

Related Commands

Command	Description
ip multicast hardware-switching replication-mode	Switches hardware replication mode among auto-detection and ingress and egress replication.

ip multicast hardware-switching replication-mode

To switch hardware replication mode among auto-detection and ingress and egress replication, use the ip multicast hardware-switching replication-mode command in global configuration mode. To restore the system to automatic detection mode, use the **no** form of this command.

ip multicast hardware-switching replication-mode egress | ingress
no ip multicast hardware-switching replication-mode egress | ingress

Syntax Description

egress	Forces the system to the egress mode of replication.
ingress	Forces the system to the ingress mode of replication.

Command Default

The Supervisor Engine 720 automatically detects the replication mode based on the module types that are installed in the system. If all modules are capable of egress replication, the system uses egress-replication mode. If the supervisor engine detects the modules that are not capable of egress replication, the replication mode automatically switches to ingress replication.

If the system is functioning in the automatic-detection egress mode, and you install a module that cannot perform egress replication, the following occurs:

- The Cisco 7600 series router reverts to ingress mode.
- A system log is generated.
- A system reload occurs to revert to the old configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRE	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

This command is supported on Supervisor Engine 720, Supervisor Engine 32, Route Switching Processor 720, and compatible DFCDs.

Note During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts are purged and reinstalled. To avoid interruptions in traffic forwarding, enter the ip multicast hardware-switching replication-mode ingress command.

If you enter the **no**ip multicast hardware-switching replication-mode **egress** command, only the forced-egress mode resets and not the forced-ingress mode.

If you enter the **no**ip multicast hardware-switching replication-mode **ingress** command, only the forced-ingress mode resets and not the forced-egress mode.

Examples

This example shows how to enable the ingress-replication mode:

```
Router# enable
Router# configure terminal
Router(config)#
ip multicast hardware-switching replication-mode ingress
```

This example shows how to enable the egress-replication mode:

```
Router# enable
Router# configure terminal
Router(config)#
ip multicast hardware-switching replication-mode egress
```

This example shows how to disable the current egress-replication mode and return to automatic detection mode:

```
Router# enable
Router# configure terminal
Router(config)#
no
ip multicast hardware-switching replication-mode egress
```

Related Commands

Command	Description
ip multicast hardware-switching non-rpf aging	Configures the multicast hardware switching for rate-limiting of non-RP aging traffic.

ip multicast heartbeat

To monitor the delivery of multicast traffic for a multicast group via Simple Network Management Protocol (SNMP) traps, use the **ip multicast heartbeat**command in global configuration mode. To disable the monitoring of multicast traffic for a multicast group, use the **no** form of this command.

ip multicast heartbeat vrf *vrf-name group-address minimum-number-intervals window-size seconds*
no ip multicast heartbeat vrf *vrf-name group-address*

Syntax Description

vrf	(Optional) Supports the Multicast VPN Routing and Forwarding (MVRF) instance.
vrf	(Optional) Name assigned to the VRF.
group-address	A multicast group Class D address, from 224.0.0.0 to 239.255.255.255.
minimum-number-intervals	Minimum number of intervals where a multicast heartbeat must be present. The range is from 1 to 100. **Note** The value specified for this argument must be less than or equal to the value specified for the *window-size* argument.
window-size	Number of intervals to monitor for a multicast heartbeat. The range is from 1 to 100. **Note** The value specified for this argument must be greater than or equal to the value specified for the *minimum-number-intervals* argument.
seconds	Length of an interval. The range is from 10 to 3600 seconds. **Note** The value entered for the *seconds*argument must be a multiple of 10.

Command Default

The monitoring of multicast traffic delivery via SNMP traps is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
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

Use the **ip multicast heartbeat** command to configure a multicast router to send SNMP traps to a network management station (NMS) when multicast source traffic being sent to a multicast group fails to meet certain multicast delivery parameters.

When this command is configured, the router monitors multicast source traffic destined to the multicast group address specified for the *group-address* argument for the number of seconds configured for the *seconds*argument (the interval). The number of packets present in the interval is not as important as whether any multicast source packets destined to the group were forwarded at all during the interval. A "heartbeat" is present if at least one source packet sent to the group was forwarded during the interval.

Note A multicast heartbeat is determined by the counter of both the (*, G) and the (S, G) state of a group being tracked. An increment in the counters of any such state is considered to constitute forwarding for the group within the interval.

In addition to the required *seconds*argument value, two other required parameters must be configured: a value for the *minimum-number-intervals* argument and a value for the *window-size*argument. The *minimum-number-intervals* argument is used to specify the minimum number of intervals where a multicast heartbeat must be present. The *window-size* argument is used to specify the number of intervals to monitor for a multicast heartbeat (the interval window).

If the router detects a heartbeat in fewer intervals than the minimum, after the interval window, an SNMP trap would be sent from this router to an NMS. The SNMP trap is used to indicate a loss of heartbeat. The SNMP trap triggered by this command is ciscoIpMRouteMissingHeartBeats, which is defined in CISCO-IPMROUTE-MIB.

The **ip multicast heartbeat**command will not create a multicast forwarding state in the router. Use the **ip igmp static-group** command on the router or on a downstream router to force forwarding of IP multicast traffic.

Use the **snmp-server enable traps** command with the **ipmulticast** keyword to enable the generation of traps associated with multicast heartbeat monitoring. Use the **snmp-server host** command to configure the sending of IP multicast traps to specific receiver hosts.

Use the **debug ip mhbeat** command to enable debugging output for IP multicast heartbeat monitoring.

Examples

The following example shows how to configure a multicast router to send SNMP traps to an NMS when multicast source traffic being sent to the multicast group fails to meet certain multicast delivery parameters. In this example, a multicast router is configured to monitor the packets forwarded for group 239.1.1.53 in intervals of 10 seconds. If at least one packet is forwarded during two out of the last five intervals (the interval window), an SNMP trap will not be generated. An SNMP trap would be generated only if the router did not see packets forwarded during three or more of the 10-second intervals within the interval window of five samples.

```
snmp-server enable traps ipmulticast
ip multicast heartbeat 239.1.1.53 2 5 10
```

Related Commands

Command	Description
debug ip mhbeat	Enables debugging output for IP multicast heartbeat monitoring.
ip igmp static-group	Configures static group membership entries on an interface.
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification operation.

ip multicast helper-map

To allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks, use the **ip multicast helper-map**command in interface configuration mode. To disable this function, use the **no** form of this command.

ip multicast helper-map *group-address broadcast-address* | **broadcast** *multicast-address access-list* [**ttl** *remapping-value*]
no ip multicast helper-map *group-address broadcast-address* | **broadcast** *multicast-address access-list* [**ttl** *remapping-value*]

Syntax Description

group-address	Multicast group address of traffic to be converted to broadcast traffic. Use this value with the *broadcast-address* value.
broadcast-address	Address to which broadcast traffic is sent. Use this value with the *group-address* value.
broadcast	Specifies the traffic to be converted from broadcast to multicast. Use this keyword with the *multicast-address* value.
multicast-address	IP multicast address to which the converted traffic is directed. Use this value with the **broadcast** keyword.
access-list	IP extended access list number or name that controls which broadcast packets are translated, based on the User Datagram Protocol (UDP) port number.
ttl *remapping-value*	(Optional) Configures the Time-to-Live (TTL) value of multicast packets generated by the helper-map from incoming broadcast packets. Valid values are from 1 to 50 hops. The default TTL value is 1 hop.

Command Default

No conversion between broadcast and multicast occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720. The **ttl** keyword and *remapping-value* arguments were added.
12.4(6)T	The **ttl** keyword and *remapping-value* arguments were added.
12.4(7)	The **ttl** keyword and *remapping-value* arguments were added.
12.3(19)	The **ttl** keyword and *remapping-value* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When a multicast-capable internetwork is between two broadcast-only internetworks, you can convert broadcast traffic to multicast at the first hop router, and convert it back to broadcast at the last hop router before delivering the packets to the broadcast clients. However, broadcast packets with the IP source address of 0.0.0.0 (such as a Dynamic Host Configuration Protocol [DHCP] request) will not be translated to any multicast group. Thus, you can take advantage of the multicast capability of the intermediate multicast internetwork. This feature prevents unnecessary replication at the intermediate routers and allows multicast fast switching in the multicast internetwork.

If you need to send a directed broadcast to the subnet, the outgoing interface of the last hop router can be configured with an IP broadcast address of x.x.x.255, where x.x.x.0 is the subnet that you are trying to reach; otherwise, the packet will be converted to 255.255.255.255.

By default, many broadcast applications use a default TTL value of 1. Because the helper-map applies the decremented TTL value of the incoming broadcast packet for the generated multicast packet, and most broadcast applications use a TTL value of 1 hop, broadcast packets may not be translated to multicast packets, and thus, may be dropped rather than forwarded. To circumvent this potential issue, you can manually configure the TTL value for broadcast packets being translated into multicast packets using the **ttl** keyword and *remapping-value* argument. For the *remapping-value* argument, specify a value that will enable the translated packets to reach multicast receivers.

Examples

The following example shows how to allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks.

In this example, assume that a server on the LAN connected to the Ethernet interface 0 of the first hop router is sending a UDP broadcast stream with a source address of 126.1.22.199 and a destination address of 126.1.22.255:4000. Based on that scenario, the configuration on the first hop router converts the broadcast stream arriving at incoming Ethernet interface 0 destined for UDP port 4000 to a multicast stream. The access list permits traffic being sent from the server at 126.1.22.199 being sent to 126.1.22.255:4000. The traffic is sent to group address 239.254.2.5. The ip forward-protocol command specifies the forwarding of broadcast messages destined for UDP port 4000.

The second configuration on the last hop router converts the multicast stream arriving at incoming Ethernet interface 1 back to broadcast at outgoing Ethernet interface 2. Again, not all multicast traffic emerging from the multicast cloud should be converted from multicast to broadcast, only the traffic destined for 126.1.22.255:4000.

The configurations for the first and last hop routers are as follows:

First Hop Router Configuration

```
interface ethernet 0
 ip address 126.1.22.1 255.255.255.0
 ip pim sparse-mode
 ip multicast helper-map broadcast 239.254.2.5 105
access-list 105 permit udp host 126.1.22.199 host 126.1.22.255 eq 4000
ip forward-protocol udp 4000
```

Last Hop Router Configuration

```
interface ethernet 1
 ip address 126.1.26.1 255.255.255.0
 ip pim sparse-mode
```

```
 ip multicast helper-map 239.254.2.5 126.1.28.255 105
interface ethernet 2
 ip address 126.1.28.1 255.255.255.0
 ip directed-broadcast
access-list 105 permit udp host 126.1.22.199 any eq 4000
ip forward-protocol udp 4000
```

Related Commands

Command	Description
ip directed-broadcast	Enables the translation of directed broadcast to physical broadcasts.
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip multicast limit

To configure per interface multicast route (mroute) state limiters, use the **ip 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.

ip multicast limit [**connected** | **out** | **rpf**] *access-list max-entries*
no ip multicast limit [**connected** | **out** | **rpf**] *access-list max-entries*

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 accounting each time that an mroute permitted by the ACL is created or deleted.
out	(Optional) Limits mroute outgoing interface list (olist) membership on an outgoing interface for an ACL-classified set of multicast traffic by accounting each time that an mroute olist member permitted by the ACL is added or removed.
rpf	(Optional) Limits the number of mroute states created for an ACL-classified set of multicast traffic on an incoming (RPF) interface by accounting each time an mroute permitted by the ACL is created or deleted.
access-list	Number or name identifying the ACL that defines the set of multicast traffic to be applied to a per interface mroute state limiter.
max-entries	Maximum number of mroutes permitted by the per interface mroute state limiter. The range is from 0 to 2147483647.

Command Default

No per interface mroute state limiters are configured.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

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

The following forms of the **ip multicast limit**command are available to configure per interface mroute state limiters:

- **ip multicast limit** *access-list max-entries*

This command limits mroute state creation for an ACL-classified set of traffic on an interface when the interface is an outgoing (egress) interface, and limits mroute outgoing interface list (olist) membership when the interface is an incoming (ingress) Reverse Path Forwarding (RPF) interface.

This type of per interface mroute state limiter limits mroute state creation--by accounting each time an mroute permitted by the ACL is created or deleted--and limits mroute olist membership--by accounting each time that an mroute olist member permitted by the ACL is added or removed.

Use the **ip multicast limit** command without the optional keywords to limit mroute state creation for an ACL-classified set of traffic on an interface when the interface is an outgoing (egress) interface, and to limit mroute olist membership when the interface is an incoming (ingress) Reverse Path Forwarding (RPF) interface. This type of mroute state limiter limits mroute state creation by accounting each time an mroute permitted by the ACL is created or deleted and limits mroute olist membership by accounting each time that an mroute olist member permitted by the ACL is added or removed. Entering this form of the command (that is, with no optional keywords) is equivalent to specifying the **ip multicast limit rpf**and **ip multicast limit out** forms of the command.

- **ip multicast limit connected** *access-list max-entries*

This command limits mroute state creation for an ACL-classified set of multicast traffic on an incoming (RPF) interface that is directly connected to a multicast source by accounting each time that an mroute permitted by the ACL is created or deleted.

- **ip multicast limit out** *access-list max-entries*

This command limits mroute olist membership on an outgoing interface for an ACL-classified set of multicast traffic by accounting each time that an mroute olist member permitted by the ACL is added or removed.

- **ip multicast limit rpf** *access-list max-entries*

This command limits mroute state creation for an ACL-classified set of multicast traffic on an incoming (RPF) interface by accounting each time an mroute permitted by the ACL is created or deleted.

For the required *access-list* argument, specify the ACL that defines the IP multicast traffic to be limited on an interface. A standard or extended ACL can be specified. Standard ACLs can be used to define the (*, G) state to be limited on an interface. Extended ACLs can be used to define the (S, G) state to be limited on an interface. Extended ACLs also can be used to define the (*, G) state to be limited on an interface, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list.

Mechanics of Per Interface Mroute State Limiters

The mechanics of per interface mroute state limiters are as follows:

- Each time the state for an mroute is created or deleted and each time an olist member is added or removed, the Cisco IOS software searches for a corresponding per interface mroute state limiter that matches the mroute.
- In the case of the creation and deletion of mroutes, the Cisco IOS software searches for a per interface mroute state limiter configured on the incoming (RPF) interface that matches the mroute to be created or deleted. In the case of olist member addition or removal, the Cisco IOS software searches for a per interface mroute state limiter configured on the outgoing interface that matches the mroute to be added or removed.

- The Cisco IOS software performs a top-down search from the list of configured per interface mroute state limiters. Only per interface mroute state limiters that match the direction of traffic are considered. The first per interface mroute state limiter that matches is used for limiting (sometimes referred to as *accounting*). A match is found when the ACL permits the mroute state.
- When a match is found, the counter of the per interface mroute state limiter is updated (increased or decreased). If no per interface mroute state limiter is found that matches an mroute, no accounting is performed for the mroute (because there is no counter to update).
- The amount to update the counter with is called the *cost* (sometimes referred to as the *cost multiplier*). The default cost is 1.

Note A per interface mroute state limiter always allows the deletion of an mroute or the removal of an interface from the olist. In those cases, the respective per interface mroute state limiter decreases the counter by the value of the cost multiplier. In addition, RPF changes to an existing mroute are always allowed (in order to not affect existing traffic). However, a per interface mroute state limiter *only* allows the creation of an mroute or the addition of an mroute olist member if adding the cost does not exceed the maximum number of mroutes permitted.

Tips for Configuring Per Interface Mroute State Limiters

- To ensure that all mroutes are accounted, you can configure a per interface mroute state limiter whose ACL contains a **permit any** statement and set the maximum for the *max-entries* argument to 0. Configuring an mroute state limiter in this manner effectively denies all fall through states, which may be a way to prevent a multicast DoS attack in and out of the interface.
- When creating an ACL, remember that, by default, the end of the ACL contains an implicit **deny any** statement for everything if it did not find a match before reaching the end.
- An explicit deny statement for a specific mroute in an ACL can be used to specify the state that will not match the ACL (thus, preventing the ACL from being accounted). If an mroute matches a deny statement, the search immediately continues to the next configured mroute state limiter. Configuring an explicit deny statement in an ACL can be more efficient than forcing the mroute to fall through an ACL (by means of the implicit **deny any** statement at the end of the ACL).

Examples

The following example shows the configuration of per interface mroute state limiters. In this example, a service provider uses per interface mroute state limiters to provide a multicast Call Admission Control (CAC) in a network environment where all the multicast flows utilize the same amount of bandwidth. The service provider configures three mroute state limits on Gigabit Ethernet interface 0/0 to provide the multicast CAC needed to provision an interface for Standard Definition (SD) channel bundles being offered to subscribers:

- An mroute state limit of 75 for the SD channels that match acl-basic.
- An mroute state limit of 25 for the SD channels that match acl-premium.
- An mroute state limit of 25 for the SD channels that match acl-gold.

```
interface GigabitEthernet0/0
description --- Interface towards the DSLAM ---
.
```

```
.
.
ip multicast limit out acl-basic 75
ip multicast limit out acl-premium 75
ip multicast limit out acl-gold 25
```

Related Commands

Command	Description
clear ip multicast limit	Resets the exceeded counter for per interface mroute state limiters.
debug ip mrouting limits	Displays debugging information about configured per interface mroute state limiters and bandwidth-based multicast CAC policies.
ip multicast limit cost	Applies costs to mroute state limiters.
show ip multicast limit	Displays statistics about configured per interface mroute state limiters.

ip multicast limit cost

To apply a cost to mroutes that match per interface mroute state limiters, use the **ip 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.

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

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the cost be applied only to mroutes associated with the Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
access-list	Extended or standard access control list (ACL) name or number 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 no **ip multicast limit cost** commands are 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 **ip 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)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use this command to apply a cost to mroutes that match per interface mroute state limiters (configured with the **ip 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.

ACLs are used with this command to define the IP multicast traffic for which to apply a cost. Standard ACLs can be used to define the (*, G) state. Extended ACLs can be used to define the (S, G) state. Extended ACLs also can be used to define the (*, G) state, by specifying 0.0.0.0 for the source address and source wildcard--referred to as (0, G)--in the permit or deny statements that compose the extended access list.

Bandwidth-based CAC policies are used with per interface mroute state limiters. Bandwidth-based CAC policies provide the capability to define costs (globally or per MVRF instance) to be applied to mroutes that

are being limited by an mroute state limiter. The *cost-multiplier* argument is used to specify the cost to apply to mroutes that match the ACL specified for the *access-list* argument.

Mechanics of the Bandwidth-Based Multicast CAC Policies

- Once an mroute matches an ACL configured for a per interface mroute state limiter, the Cisco IOS software performs a top-down search from the global or per MVRF list of configured bandwidth-based multicast CAC policies to determine if a cost should be applied to the mroute.
- A cost is applied to the first bandwidth-based CAC policy that matches the mroute. A match is found when the ACL applied to the bandwidth-based CAC policy permits the mroute state.
- The counter for the mroute state limiter either adds or subtracts the cost configured for the *cost-multiplier* argument. If no costs are configured or if the mroute does not match any of the configured bandwidth-based CAC polices, the default cost of 1 is used.

Tips for Configuring Bandwidth-Based CAC Policies for IP Multicast

- To ensure that a particular cost applies to all mroutes being limited, you can configure a bandwidth-based CAC policy whose ACL contains a **permit any** statement. Configuring a bandwidth-based CAC policy in this manner effectively ensures that the default cost is not applied to any mroutes being limited.
- Configuring a bandwidth-based CAC policy with a cost of 0 for the *cost-multiplier* argument can be used to skip the accounting of certain mroutes (for example, to prevent Auto-RP groups or a specific multicast channel from being accounted).
- An explicit deny statement for a specific mroute in an ACL can be used to specify the state that will not match the ACL (thus, preventing the ACL from being accounted). If an mroute matches a deny statement, the search immediately continues to the next configured bandwidth-based CAC policy. Configuring an explicit deny statement in an ACL can be more efficient than forcing the mroute to fall through an ACL (by means of the implicit **deny any** statement at the end of the ACL).

Examples

The following example shows a bandwidth-based multicast CAC policy configuration. In this example, a service provider uses per interface mroute state limiters with bandwidth-based multicast CAC policies to provision Gigabit Ethernet interface 0/0 for the fair sharing of bandwidth required between three content providers.

```
!
interface GigabitEthernet0/0
 ip multicast limit out acl-CP1-channels 250000
 ip multicast limit out acl-CP2-channels 250000
 ip multicast limit out acl-CP3-channels 250000
!
!
ip multicast limit cost acl-MP2SD-channels 4000
ip multicast limit cost acl-MP2HD-channels 18000
ip multicast limit cost acl-MP4SD-channels 1600
ip multicast limit cost acl-MP4HD-channels 6000
!
.
.
.
!
interface GigabitEthernet0/0
 ip multicast limit out acl-CP1-channels 250000
 ip multicast limit out acl-CP2-channels 250000
```

```
 ip multicast limit out acl-CP3-channels 250000
!
```

Related Commands

Command	Description
ip multicast limit	Configures per interface mroute state limiters.

ip multicast mrinfo-filter

To filter multicast router information (mrinfo) request packets, use the **ip multicast mrinfo-filter**command in global configuration mode. To remove the filter on mrinfo requests, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **mrinfo-filter** *access-list*
no ip multicast [**vrf** *vrf-name*] **mrinfo-filter**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
access-list	IP standard numbered or named access list that determines which networks or hosts can query the local multicast router with the **mrinfo** command.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for 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

The **ip multicast mrinfo-filter**command filters the mrinfo request packets from all of the sources denied by the specified access list. That is, if the access list denies a source, that source's mrinfo requests are filtered. mrinfo requests from any sources permitted by the ACL are allowed to proceed.

Examples

The following example shows how to filter mrinfo request packets from all hosts on network 192.168.1.1 while allowing requests from any other hosts:

```
ip multicast mrinfo-filter 51
access-list 51 deny 192.168.1.1
access list 51 permit any
```

Related Commands

Command	Description
mrinfo	Queries a multicast router about which neighboring multicast routers are peering with it.

ip multicast multipath

To enable load splitting of IP multicast traffic over Equal Cost Multipath (ECMP), use the **ip multicast multipath**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash basic** | **next-hop-based**]
no ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash basic** | **next-hop-based**]

Syntax Description

vrf *vrf-name*	(Optional) Enables ECMP multicast load splitting for IP multicast traffic associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
s-g-hash	(Optional) Enables ECMP multicast load splitting based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords: • **basic** --Enables a simple hash based on source and group address. This algorithm is referred to as the basic S-G-hash algorithm. • **next-hop-based** --Enables a more complex hash based on source, group, and next-hop address. This algorithm is referred to as the next-hop-based S-G-hash algorithm.

Command Default

If multiple equal-cost paths exist, multicast traffic will not be load split across those paths.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name*argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SRB	This command was modified. The **s-g-hash**, **basic**, and **next-hop-based** keywords were added in support of the IP Multicast Load Splitting--Equal Cost Multipath (ECMP) Using S, G and Next Hop feature.
15.0(1)M	This command was modified. The **s-g-hash**, **basic**, and **next-hop-based** keywords were added in support of the IP Multicast Load Splitting--Equal Cost Multipath (ECMP) Using S, G and Next Hop feature.
15.0(1)S	This command was integrated into Cisco IOS Release15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **ip multicast multipath** command to enable load splitting of IP multicast traffic across multiple equal-cost paths.

If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.

Configuring load splitting with the **ip multicast multipath** command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.

Note The **ip multicast multipath**command load splits the traffic but does not *load balance* the traffic. Traffic from a source will use only one path, even if the traffic far outweighs traffic from other sources.

If the **ip multicast multipath** command is configured with the **s-g-hash** keyword and multiple equal-cost paths exist, load splitting will occur across equal-cost paths based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords:

- **basic** --Enables a simple hash based on source and group address. The basic S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. The basic S-G-hash algorithm, however, is subject to polarization because for a given source and group, the same hash is always picked irrespective of the router the hash is being calculated on.
- **next-hop-based** --Enables a more complex hash based on source, group, and next-hop address. The next-hop-based S-G-hash algorithm is predictable because no randomization is used in coming up with the hash value. Unlike the S-hash and basic S-G-hash algorithms, the next-hop-based hash mechanism is not subject to polarization.

Examples

The following example shows how to enable ECMP multicast load splitting on a router based on source address using the S-hash algorithm:

```
ip multicast multipath
```

The following example shows how to enable ECMP multicast load splitting on a router based on source and group address using the basic S-G-hash algorithm:

```
ip multicast multipath s-g-hash basic
```

The following example shows how to enable ECMP multicast load splitting on a router based on source, group, and next-hop address using the next-hop-based S-G-hash algorithm:

```
ip multicast multipath s-g-hash next-hop-based
```

ip multicast oif-per-mvrf-limit

To configure the limit for the total number of outgoing interfaces (OIFs) per Multicast VPN Routing and Forwarding (MVRF) instance, use the **ip multicast oif-per-mvrf-limit** command in global configuration mode. To reset the limit for number of OIFs per MVRF, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **oif-per-mvrf-limit** *number* [*threshold* | [**turn-off-pim**] | **turn-off-pim**]

no ip multicast [**vrf** *vrf-name*] **oif-per-mvrf-limit** *number* [*threshold* | [**turn-off-pim**] | **turn-off-pim**]

Syntax Description

vrf	(Optional) Supports the MVRF instance.
vrf-name	(Optional) Name assigned to the VRF.
number	Total number of OIFs per MVRF. The range is from 1 to 2147483647.
threshold	(Optional) Threshold at which a warning message is generated. The range is from 1 to 2147483647.
turn-off-pim	(Optional) Turns off Protocol Independent Multicast (PIM) on all MVRF interfaces while reaching the limit for total number OIFs in an MVRF.

Command Default

No limit is set for number of OIFs in an MVRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S3	This command was introduced.

Usage Guidelines

Use the **ip multicast oif-per-mvrf-limit** command to configure the limit for the total number of OIFs in an MVRF.

When the total number of OIFs present in the MVRF exceeds the configured threshold value, the system generates a message to report it. When the total number of OIFs exceeds the configured limit, additional OIFs cannot be added in any multicast route (mroute) state of the MVRF.

When you configure the **turn-off-pim** option and the total number of OIFs present in the MVRF exceeds the configured limit for number of OIFs in an MVRF, PIM control packets are not sent out and the router does not process the received PIM control packets.

Examples

The following example shows how to limit the total number of OIFs in an MVRF to 3000 in the default MVRF and set the threshold value to 2500 to generate a warning message on the console and turn off PIM:

```
Router(config)# ip multicast oif-per-mvrf-limit 3000 2500 turn-off-pim
```

Related Commands

Command	Description
ip multicast total-oif-limit	Configures the limit for the total number of OIFs in a router.

ip multicast rate-limit

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip multicast rate-limit**command is not available in Cisco IOS software.

To control the rate at which a sender from the source list can send to a multicast group in the group list, use the **ip multicast rate-limit**command in interface configuration mode. To remove the control, use the **no** form of this command.

ip multicast rate-limit in | **out** [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*
no ip multicast rate-limit in | **out** [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

Syntax Description

in	Accepts only packets at the rate of the value for the *kbps* argument or slower on the interface.
out	Sends only a maximum of the value for the *kbps* argument on the interface.
video	(Optional) Performs rate limiting based on the User Datagram Protocol (UDP) port number used by video traffic. Video traffic is identified by consulting the Session Announcement Protocol (SAP) cache.
whiteboard	(Optional) Performs rate limiting based on the UDP port number used by whiteboard traffic. Whiteboard traffic is identified by consulting the SAP cache.
group-list *access-list*	(Optional) Specifies the access list number or name that controls which multicast groups are subject to the rate limit.
source-list *access-list*	(Optional) Specifies the access list number or name that controls which senders are subject to the rate limit.
kbps	Transmission rate (in kbps). Any packets sent at greater than this value are discarded. The default value is 0, meaning that no traffic is permitted. Therefore, set this to a positive value.

Command Default

If this command is not configured, there is no rate limit. If this command is configured, the *kbps* value defaults to 0, meaning that no traffic is permitted.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

If a router receives a packet the user has sent over the limit, the packet is dropped; otherwise, it is forwarded.

For the **video** or **whiteboard** keyword to work, the **ip sap listen** command must be enabled so that the port number can be obtained from the SAP cache. If the **ip sap listen** command is not enabled, or the group address is not in the SAP cache, no rate-limiting is done for the group.

Examples

In the following example, packets to any group from sources in network 172.16.0.0 will have their packets rate-limited to 64 kbps:

```
interface serial 0
 ip multicast rate-limit out group-list 1 source-list 2 64
access-list 1 permit 0.0.0.0 255.255.255.255
access-list 2 permit 172.16.0.0 0.0.255.255
```

Related Commands

Command	Description
ip sap listen	Enables the Cisco IOS software to listen to session directory advertisements.

ip multicast redundancy routeflush maxtime

To configure an additional timeout period before stale forwarding plane multicast routing (mroute) information is flushed following a Route Processor (RP) switchover, use the **ip multicast redundancy routeflush maxtime** command in global configuration mode. To restore the default with respect to the command, use the **no** form of this command.

ip multicast redundancy routeflush maxtime *seconds*
no ip multicast redundancy routeflush maxtime

Syntax Description

seconds	Timeout period, in seconds. The range is from 0 to 3600.

Command Default

The default nonstop forwarding (NSF) route flush time is 30 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **ip multicast redundancy routeflush maxtime** command to configure an additional timeout period before stale forwarding plane mroute information is flushed. This timeout period is added on to the default nonstop forwarding (NSF) route flush time as a delay between the downloading of refreshed multicast control plane route information to the forwarding plane and the flushing of "stale" NSF forwarding plane information retained from a stateful switchover (SSO) before the RP switchover.

Caution It is not recommended that you configure this additional delay unless it is specifically required for your topology because it could increase the risk of routing loops during NSF.

Note You would need to invoke this command only if you have a routing protocol that requires additional time to populate routing information after the signaling of unicast routing convergence (for example, Border Gateway Protocol [BGP] in a configuration with a large number of VPN routing and forwarding [VRF] instances). The need to configure this timeout period may be determined during predeployment SSO stress testing.

Use the **show ip multicast redundancy state**command to display the current redundancy state for IP multicast. The output from this command can be used to confirm the NSF state flush timeout period being used.

Examples

The following example shows how to configure an additional timeout period of 900 seconds (15 minutes) before stale forwarding plane mroute information is flushed:

```
Router
(config)
```

```
#
 ip multicast redundancy routeflush maxtime 900
```

Related Commands

Command	Description
show ip multicast redundancy state	Displays information about the current redundancy state for IP multicast.

ip multicast route-limit

To limit the number of multicast routes (mroutes) that can be added to a multicast routing table, use the **ip multicast route-limit**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]
no ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
limit	The number of mroutes that can be added. The range is from 1 to 2147483647. The default is 2147483647.
threshold	(Optional) The number of mroutes that cause a warning message to occur. The threshold value must not exceed the limit value.

Command Default

limit : 2147483647

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Releaes 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded. If the user sets the *threshold* argument, a threshold error message is generated when the threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the *limit* argument.

The mroute warning threshold must not exceed the mroute limit.

Examples

The following example shows how to set the mroute limit to 200,000 and the threshold to 20,000 mroutes for a VRF instance named test:

```
ip multicast vrf test route-limit 200000 20000
```

ip multicast rpf backoff

To configure the intervals at which Protocol Independent Multicast (PIM) Reverse Path Forwarding (RPF) failover will be triggered by changes in the routing tables, use the ip multicast rpf backoff command in global configuration mode. To set the triggered RPF check to the default values, use the no form of this command.

ip multicast rpf backoff *minimum maximum* [**disable**]
no ip multicast rpf backoff *minimum maximum* [**disable**]

Syntax Description

minimum	The minimum configured backoff interval. The backoff interval is reset to the number of milliseconds (ms) configured by the *minimum* argument if a backoff interval has expired without any routing changes. The default is 500 milliseconds (ms).
maximum	The maximum amount of time, in milliseconds, allowed for a backoff interval. The maximum length of time that is allowed is 5000 ms. The default is 5000 ms.
disable	(Optional) Turns off the triggered RPF check function.

Command Default

This command is enabled by default.*minimum*: 500 ms.*maximum*: 5000 ms.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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

In an unstable unicast routing environment that uses triggered RPF checks, the environment could be constantly triggering RPF checks, which places a burden on the resources of the router. To avoid this problem, use the **ip multicast rpf backoff** command to prevent a second triggered RPF check from occurring for the length of time configured. That is, the PIM "backs off" from another triggered RPF check for a minimum amount of milliseconds as configured by the user.

If the backoff period expires without further routing table changes, PIM then scans for routing changes and accordingly establishes multicast RPF changes. However, if more routing changes occur during the backoff period, PIM doubles the backoff period to avoid overloading the router with PIM RPF changes while the routing table is still converging.

Note We recommend that users keep the default values for this command. The default values allow subsecond RPF failover.

The *maximum* argument is used to configure the maximum backoff interval. The backoff time is reset to the time configured by the *minimum* argument if an entire backoff interval has expired without routing changes.

The *maximum* argument default allows the RPF change behavior to be backward-compatible, allowing a 5-second RPF check interval in case of frequent route changes and a 500-ms RPF check interval in stable networks with only unplanned routing changes. Before the introduction of the **ip multicast rpf backoff** command, PIM polled the routing tables for changes every 5 seconds.

You likely need not change the defaults of the **ip multicast rpf backoff**command unless you have frequent route changes in your router (for example, on a dial-in router). Changing the defaults can allow you to reduce the maximum RPF check interval for faster availability of IP multicast on newly established routes or to increase the maximum RPF check interval to reduce the CPU load caused by the RPF check.

Examples

The following example shows how to set the minimum backoff interval to 100 ms and the maximum backoff interval to 2500 ms:

```
ip multicast rpf backoff 100 2500
```

ip multicast rpf interval

To modify the intervals at which periodic Reverse Path Forwarding (RPF) checks occur, use the **ip multicast rpf interval** command in global configuration mode. To return to the default interval, use the no form of this command.

ip multicast rpf interval *seconds* [**list** *access-list* | **route-map** *route-map*]
no ip multicast rpf interval *seconds* [**list** *access-list* | **route-map** *route-map*]

Syntax Description

seconds	The number of seconds at which the interval is configured. The default is 10 seconds.
list *access-list*	(Optional) Defines the interval of periodic RPF checks for an access list.
route-map *route-map*	(Optional) Defines the interval of periodic RPF checks for a route map.

Command Default

This command is enabled by default.*seconds*: 10

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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

You can configure multiple instances of this command by using an access list or a route map.

Note We recommend that users keep the default values for this command. The default values allow subsecond RPF failover.

Examples

The following example shows how to set the periodic RPF check interval to 10 seconds:

```
ip multicast rpf interval 10
```

The following example shows how to set the periodic RPF check interval for groups that are defined by access list 10 to 3 seconds:

```
ip multicast rpf interval 3 list 10
```

The following example shows how to set the periodic RPF check interval for groups that are defined by the route map named map to 2 seconds:

```
ip multicast rpf interval 2 route-map map
```

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host hello messages.

ip multicast rpf mofrr

To enable a Provider Edge (PE) router to perform Reverse Path Forwarding (RPF) lookups using multicast only fast re-route (MoFRR) on an IP address of the exit router in the global table or a specific VPN, use the **ip multicast rpf mofrr**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **rpf mofrr access-list-number** | **access-list-name** [**sticky**]
no ip multicast [**vrf** *vrf-name*] **rpf mofrr access-list-number** | **access-list-name** [**sticky**]

Syntax Description

vrf *vrf-name*	(Optional) Enables a PE router to perform an RPF lookup using MoFRR on the exit router for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
access-list-name	Name of the IP access list or object group access control list (OGACL). Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access control list (ACL). MoFRR is enabled for the mroute matching the ACL. • An extended IP access list is in the range 100 to 199 or 2000 to 2699. **Note** MoFRR accepts extended ACLs only. It does not accept standard ACLs.
sticky	(Optional) Ensures that the primary RPF does not change even if a better primary comes along. It changes only if for some reason the current primary RPF is unreachable. The sticky keyword ensures that there is no RPF flapping happening on mroutes if the unicast routes are fluctuating for some reason.

Command Default

The RPF MoFRR functionality is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use the **ip multicast rpf mofrr** command to enable a PE router to perform RPF lookups using MoFRR on an IP address of the exit router in the global table or a specific VPN. MoFRR uses standard Protocol Independent Multicast (PIM) join messages to set up a primary and a secondary multicast forwarding path by establishing a primary and a secondary RPF interface on each router that receives a PIM join message. Data is received from both the primary and backup paths. If the router detects a forwarding error in the primary path, it switches RPF to the secondary path and immediately has packets available to forward out to each outgoing interface.

MoFRR accepts extended ACLs only. It does not accept standard ACLs.

Examples

The following example shows how to enable a PE router to perform RPF lookups using MoFRR for the mroute matching the ACL numbered 150:

```
ip multicast rpf mofrr 150
```

Related Commands

Command	Description
show ip mroute	Displays information about the multicast routing (mroute) table.
show ip rpf	Displays the information that IP multicast routing uses to perform the RPF check for a multicast source.

ip multicast rpf proxy vector

To enable a provider edge (PE) router to perform a Reverse Path Forwarding (RPF) check on an IP address of the exit router in the global table or a specific VPN, use the **ip multicast rpf proxy vector**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] [**disable**] **vector**
no ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] [**disable**] **vector**

Syntax Description

vrf *vrf-name*	(Optional) Enables a PE router to perform an RPF check on the exit router for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument. **Note** The **rd** keyword is required if the **vrf** keyword and *vrf-name* argument are entered.
rd	(Optional) Enables the route distinguisher (RD) vector in MVPN inter-AS Option B deployments. **Note** In an Option B deployment, you must enter the **ip multicast rpf proxy** command with the **rd** keyword for MVPN inter-AS support. The **rd** keyword is not required for MVPN inter-AS support Option C deployments.
disable	(Optional) Rejects the Protocol Independent Multicast (PIM) proxy and attribute RPF information.
vector	Enables the Border Gateway Protocol (BGP) next-hop as vector in PIM join messages.

Command Default

The RPF Vector functionality is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **ip multicast rpf proxy vector** command to enable a PE router to perform an RPF check on an IP address of the exit router in the global table or a specified VPN.

Use the **rd** keyword to configure PE routers to include the RD value of the VPN associated with the PIM RPF Vector encoding inserted into PIM join and prune messages. Because ASBRs in MVPN Option B deployments

change the next hop of the originating PE router for a given MDT group, including the RD value in the PIM RPF Vector encoding enables the ASBR to perform a lookup on the RD value for a prefix, which, in turn, enables the ASBR to identify which VPN the RPF Vector is intended for.

RPF Vector Functionality

Normally, in an MVPN environment, PIM sends join messages containing the IP address of upstream PE routers that are sources of a given Multicast Distribution Tree (MDT) group. To be able to perform RPF checks, however, provider (P) routers must have IPv4 reachability to source PE routers in remote autonomous systems. This behavior is not the case with inter-AS Options B and C (defined in RFC 4364) because the autonomous systems do not exchange any of their Interior Gateway Protocol (IGP) routes, including those of their local PE routers. However, P routers do have reachability to the BGP next hop of the BGP MDT update received with the BGP MDT Subaddress Family Identifier (SAFI) updates at the PE routers. Therefore, if the PE routers add the remote PE router IP address (as received within the BGP MDT SAFI) and the BGP next-hop address of this address within the PIM join, the P routers can perform an RPF check on the BGP next-hop address rather than the original PE router address, which, in turn, allows the P router to forward the join toward the Autonomous System Border Router (ASBR) that injected the MDT SAFI updates for a remote autonomous system. This functionality is generally referred to as the *PIM RPF Vector* ; the actual vector that is inserted into PIM joins is referred to as the *RPF Vector* or the *Proxy Vector* . The PIM RPF Vector, therefore, enables P routers to determine the exit ASBR to a source PE router in a remote autonomous system. Having received the join that contains a RPF Vector, an ASBR can then determine that the next-hop address is in fact itself and can perform an RPF check based on the originating PE router address carried in the PIM join.

RPF Vector Configuration Guidelines

When configured on PE routers using the **ip multicast rpf proxy vector** command, the RPF Vector is encoded as a part of the source address in PIM join and prune messages. The RPF Vector is the IGP next hop for PIM RPF neighbor in PIM join and prune messages, which is typically the exit ASBR router to a prefix in a remote autonomous system.

When enabling the RPF Vector on PE routers in Option B deployments, the following form of the **ip multicast rpf proxy vector** command should be used:

ip multicast vrf *vrf-name* **rpf proxy rd vector**

This form of the command enables an PE router to perform RPF checks on an IP address of the exit router for a specific VPN. The **rd** keyword is used in this form of the command to configure PE routers to include the RD value of the VPN associated with the PIM RPF Vector encoding inserted into PIM join and prune messages. Because ASBRs in Option B deployments change the next hop of the originating PE router for a given MDT group, including the RD value in the PIM RPF Vector encoding enables the ASBR to perform a lookup on the RD value for a prefix, which, in turn, enables the ASBR to identify which VPN the RPF Vector is intended for.

When enabling the RPF Vector on PE routers in Option C deployments, the following form of the **ip multicast rpf proxy vector** command should be used:

ip multicast rpf proxy vector

This form of the command enables the PE router to perform RPF checks on an IP address of the exit router in the global table.

RPF Vector Verification

Use the **show ip pim neighbor** command to verify that a PIM neighbor supports the RPF Vector functionality. The P flag in the output of the **show ip pim neighbor** command indicates that a PIM neighbor has announced (through PIM hello messages) its capability to handle RPF Vectors in PIM join messages. All Cisco IOS

versions that support the PIM RPF Vector feature announce this PIM hello option. An RPF Vector is only included in PIM messages when all PIM neighbors on an RPF interface support it.

Examples

The following example shows how to enable a PE router to perform RPF checks on the IP address of the exit router in the global table:

```
ip multicast rpf proxy vector
```

Related Commands

Command	Description
show ip pim neighbor	Displays information about PIM neighbors.

ip multicast rpf select

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

ip multicast [**vrf** *receiver-vrf-name*] **rpf select global** | **vrf** *source-vrf-name* **group-list** *access-list*
no ip multicast [**vrf** *receiver-vrf-name*] **rpf select global** | **vrf** *source-vrf-name* **group-list** *access-list*

Syntax Description

vrf *receiver-vrf-name*	(Optional) Applies a group-based VRF selection policy to RPF lookups originating in the MVRF specified for the *receiver-vrf-name* argument. If the optional **vrf** keyword and *receiver-vrf-name* argument are not specified, the group-based VRF selection policy applies to RPF lookups originating in the global table.
global	Specifies that the RPF lookup for groups matching the access control list (ACL) specified for the **group-list** keyword and *access-list* argument be performed in the global routing table.
vrf *source-vrf-name*	Specifies that the RPF lookups for groups matching the ACL specified with the **group-list** keyword and *access-list* argument be performed in the VRF specified for the *vrf-name* argument.
group-list *access-list*	Specifies the ACL to be applied to the group-based VRF selection policy.

Command Default

No group-based VRF selection policies are configured.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

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

This command uses the permit clauses of an 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 **ip 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 ip rpf select** command after configuring group-based VRF selection policies to display group-to-VRF mapping information.

Use the **show ip rpf** command to display how IP multicast does RPF.

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-A instead of the global table:

```
ip multicast rpf select vrf VPN-A group-list 1
!
.
.
.
!
access-list 1 permit 239.0.0.0 0.255.255.255
!
```

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.
show ip rpf select	Displays group-to-VRF mapping information.

ip multicast rpf select topology

To associate a multicast topology with a multicast group with a specific mroute entry, use the **ip multicast rpf select topology**command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip multicast rpf select topology multicast | **unicast** *topology-name access-list-number*
no ip multicast rpf select topology multicast | **unicast** *topology-name access-list-number*

Syntax Description

multicast	Associates a multicast topology with an (S,G) mroute entry.
unicast	Associates a unicast topology with an (S,G) mroute entry.
topology-name	Name of the topology instance.
access-list-number	Number of the access list.

Command Default

The topology is not associated with an (S,G) mroute entry.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **ip multicast rpf select topology**command associates a multicast topology with an (S,G) mroute entry. One (S,G) mroute entry can be associated with multiple topologies. During RPF lookup, PIM MT-ID will be used (smaller ID has higher priority) to select a topology.

One access list could be associated with multiple (S,G) mroute entries. The sequence number in the access list is used to determine the order of (S,G) mroute entry lookup within the access list.

One topology can be associated with only one access list.

Examples

The following example shows how to associate a multicast topology with an (S,G) mroute entry:

```
ip multicast rpf select topology multicast topology live-A 111
```

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast topology	Configures topology selection for multicast streams.
show ip multicast topology	Displays IP multicast topology information.

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing**command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**vrf** *vrf-name*] [**distributed**]
no ip multicast-routing [**vrf** *vrf-name*]

Cisco IOS XE Release 3.3S
ip multicast-routing [**vrf** *vrf-name*] **distributed**
no ip multicast-routing [**vrf** *vrf-name*] **distributed**

Syntax Description

vrf *vrf-name*	(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
distributed	(Optional) Enables Multicast Distributed Switching (MDS).

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the **no** form of this command now disables IP multicast routing on the Multicast MultiLayer Switching (MMLS) Route Processor (RP) and purges all multicast MLS cache entries on the MMLS-SE.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S. This command without the **distributed** keyword was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.3S	This command was modified. Either the **distributed** keyword or the **vrf** *vrf-name* **distributed** keyword and argument combination is required with this command in Cisco IOS Release 3.3S.

Release	Modification
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T. The **distributed** keyword is not supported in Cisco IOS Release 15.2(3)T.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

The optional **distributed** keyword for this command is not supported in Cisco IOS XE Release 3.2S.

Either the **distributed** keyword or the **vrf** *vrf-name* **distributed** keyword and argument combination for this command is required in Cisco IOS XE Release 3.3S and later releases.

Note For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

Examples

The following example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)#
ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Router(config)#
no ip multicast-routing
```

The following example shows how to enable MDS in Cisco IOS XE Release 3.3S a specific VRF:

```
Router(config)#
ip multicast-routing vrf vrf1 distributed
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip multicast rsvp

To configure multicast Call Admission Control (CAC) functionality based on Resource Reservation Protocol (RSVP) messages, use the **ip multicast rsvp** command in global configuration mode. To return to the default, use the **no** form of this command.

```
ip  multicast [vrf vrf-name] rsvp access-list
no  ip  multicast [vrf vrf-name] rsvp access-list
```

Syntax Description

vrf *vrf-name*	(Optional) Applies the multicast group address range to group addresses associated with the specified Multicast Virtual Private Network (MVPN) routing and forwarding instance (MVRF).
access-list	Access control list (ACL) that defines the source of the data flow to be permitted or denied. Valid entries for the *access-list* argument are as follows: • A number from 1 to 199, where 1 to 99 is a standard access list and 100 to 199 is an extended access list. • An alphanumeric string for a named access list.

Command Default

Multicast data flows are not subject to RSVP multicast CAC.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Usage Guidelines

Use the **ip multicast rsvp** command to specify which multicast flows are to be blocked when no RSVP reservation is available and the flows which are to be forwarded when an RSVP reservation is available.

Use the optional **vrf** *vrf-name* keyword and argument to apply an IP multicast group address range to the MVRF instance specified by the *vrf-name* argument.

For the required *access-list* argument, specify an ACL to be subject to RSVP:

- A standard ACL can be used to define the group address range to be permitted or denied globally.
- An extended ACL is used to define (S, G) traffic to be permitted or denied globally. If an access list is extended, source/mask (applied to S) comes first and destination/mask (applied to G) comes next. Extended ACLs can also be used to define the (*, G) state to be permitted or denied globally by specifying source 0.0.0.0 for the source address in the permit statements that comprise the extended ACL. The source 0.0.0.0 corresponds to the * in (*,G), but has no other meaning than * and does not accumulate reservations for different sources of the same group.

If an administrator modifies the ACL and a previously denied flow no longer matches the filter, the flow will be permitted upon the next RSVP notification.

ACLs for the source of the data flow to be blocked or forwarded must be defined using the **ip access-list** command in global configuration mode.

In order for a device to participate in RSVP, RSVP must be enabled on the appropriate interfaces by using the **ip rsvp bandwidth** command in interface configuration mode

In order for RSVP multicast CAC to function, the preemption parameter must be enabled for RSVP by using the **ip rsvp policy preempt** command in global configuration mode.

Examples

The following example shows how to permit all flows from all devices on network 192.0.2.0 (ACL mcast-rsvp) when an RSVP reservation is available:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp policy preempt
Device(config)# ip multicast rsvp mcast-rsvp
Device(config)# ip access-list standard mcast-rsvp
Device(config-std-nacl)# permit 192.0.2.0 0.0.0.255
```

Related Commands

Command	Description
ip access-list	Defines an IP access list or object-group access control list (ACL) by name or number .
ip rsvp bandwidth	Enables RSVP on an interface.
ip rsvp policy preempt	Enables the preemption parameter for all configured local and remote policies.

ip multicast source-per-group-limit

To configure the limit for the total number of sources for a group per Multicast Virtual Routing and Forwarding (MVRF), use the **ip multicast source-per-group-limit** command in global configuration mode. To reset the limit for the total number of sources for a group per MVRF, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **source-per-group-limit** *number* [*threshold*]

no ip multicast [**vrf** *vrf-name*] **source-per-group-limit** *number* [*threshold*]

Syntax Description

vrf	(Optional) Supports the MVRF instance.
vrf-name	(Optional) Name assigned to the VRF.
number	Total number of sources for a group per MVRF. The range is from 1 to 2147483647.
threshold	(Optional) Threshold at which a warning message is generated.

Command Default

No limit is set for the total number of sources for a group.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S3	This command was introduced.

Usage Guidelines

Use the **ip multicast source-per-group-limit** command to configure the limit for the total number of sources for a group in an MVRF.

When the total number of sources present in the MVRF exceeds the configured threshold value, the system generates a message to report it, and when it exceeds the configured limit, additional states cannot be added for the group.

Examples

The following example shows how to limit the total number of sources per group to 10 in the default MVRF and the set the threshold value to 8 to generate a warning message on the console:

```
Router(config)#ip multicast source-per-group-limit 10 8
```

Related Commands

Command	Description
ip multicast oif-per-mvrf-limit	Configures the limit for the total number of OIFs per MVRF.
ip multicast total-oif-limit	Configures the limit for the total number of OIFs in a router.

ip multicast topology

To configure topology selection for multicast streams, use the **ip multicast topology**command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip multicast topology multicast | **unicast** *topology-name* **tid** *topology-number*
no ip multicast topology multicast | **unicast** *topology-name* **tid** *topology-number*

Syntax Description

multicast	Configures a multicast topology instance.
unicast	Configures a unicast topology instance.
topology-name	Name of the topology instance.
tid *topology-number*	Specifies the number of the topology identifier.

Command Default

All multicast streams are associated with the multicast base topology.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

The **ip multicast topology** command configures topology selection for multicast streams, which is usually only required for first hop and last hop routers (and may not be required for transit routers in between). The stream, specified by an extended IP access list, can be source based, group based, or a combination of both. The sequence number in the access list will decide the order of the (S,G) mroute entries.

Examples

The following example shows how to configure topology selection for multicast streams:

```
ip multicast topology multicast live-A 111
```

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast rpf select topology	Associates a multicast topology with a multicast group with a specific mroute entry.
show ip multicast topology	Displays IP multicast topology information.

ip multicast total-oif-limit

To configure the limit for the total number of outgoing interfaces (OIFs) in a router, use the **ip multicast total-oif-limit** command in global configuration mode. To reset the limit for total OIFs in a router, use the **no** form of this command.

ip multicast total-oif-limit *number* [*threshold* | [**turn-off-pim**] | **turn-off-pim**]

no ip multicast total-oif-limit *number* [*threshold* | [**turn-off-pim**] | **turn-off-pim**]

Syntax Description

number	Total number of OIFs in a router. The range is from 1 to 2147483647.
threshold	(Optional) Threshold at which a warning message is generated. The range is from 1 to 2147483647.
turn-off-pim	(Optional) Turns off Protocol Independent Multicast (PIM) on all nondefault Multicast VPN Routing and Forwarding (MVRF) interfaces when the limit for the total number of OIFs is reached.

Command Default

No limit is set for the total number of OIFs in a router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S3	This command was introduced.

Usage Guidelines

Use the **ip multicast total-oif-limit** command to configure the limit for the total number of OIFs in a router.

When the total number of OIFs present in the router exceeds the configured threshold value, the system generates a message to report it. When the number of OIFs exceeds the configured limit, the system generates another message and additional OIFs cannot be added on any MVRF in any multicast route (mroute) state.

When you configure the **turn-off-pim** keyword and the total number of OIFs present in the router exceeds the configured total OIF limit for all nondefault MVRFs, PIM control packets are not sent out and the router does not process the received PIM control packets.

Examples

The following example shows how to limit the OIF count to 80000 across all MVRFs including the default MVRF and set an OIF count threshold of 75000 for generating a warning message:

```
Router(config)#ip multicast total-oif-limit 80000 75000
```

Related Commands

Command	Description
ip multicast oif-per-mvrf-limit	Configures the limit for the total number of OIFs in an MVRF.

ip multicast ttl-threshold

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip multicast ttl-threshold**command is not available in Cisco IOS software.

To configure the time-to-live (TTL) threshold of multicast packets being forwarded out an interface, use the **ip multicast ttl-threshold** command in interface configuration mode. To return to the default TTL threshold, use the **no** form of this command.

ip multicast ttl-threshold *ttl-value*
no ip multicast ttl-threshold *ttl-value*

Syntax Description

ttl-value	Time-to-live value, in hops. It can be a value from 0 to 255. The default value is 0, which means that all multicast packets are forwarded out the interface.

Command Default

The default TTL value is 0, which means that all multicast packets are forwarded out the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	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.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

Only multicast packets with a TTL value greater than the threshold are forwarded out the interface.

You should configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

This command replaces the **ip multicast-threshold** command.

Examples

The following example sets the TTL threshold on a border router to 200, which is a very high value. In this example multicast packets must have a TTL greater than 200 in order to be forwarded out this interface. Multicast applications generally set this value well below 200. Therefore, setting a value of 200 means that no packets will be forwarded out the interface.

```
interface tunnel 0
 ip multicast ttl-threshold 200
```

ip multicast use-functional

To enable the mapping of IP multicast addresses to the Token Ring functional address 0xc000.0004.0000, use the **ip multicast use-functional**command in interface configuration mode. To disable the function, use the **no** form of this command.

ip multicast use-functional
no ip multicast use-functional

Syntax Description

This command has no arguments or keywords.

Command Default

IP multicast address are mapped to the MAC-layer address 0xFFFF.FFFF.FFFF.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is accepted only on a Token Ring interface.

Neighboring devices on the Token Ring on which this feature is used should also use the same functional address for IP multicast traffic.

Because there are a limited number of Token Ring functional addresses, other protocols may be assigned to the Token Ring functional address 0xc000.0004.0000. Therefore, not every frame sent to the functional address is necessarily an IP multicast frame.

Examples

The following example configures any IP multicast packets going out Token Ring interface 0 to be mapped to MAC address 0xc000.0004.0000:

```
interface token 0
 ip address 10.0.0.0 255.255.255.0
 ip pim dense-mode
 ip multicast use-functional
```