ip msdp through M

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-address*| *peer-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-name*| *peer-address*} *text*

no ip msdp [**vrf** *vrf-name*] **description** {*peer-name*| *peer-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-address*| *peer-name*} [**list** *access-list*]

no ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address*| *peer-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.

Release	Modification
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 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-address*| *peer-name*}

no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address*| *peer-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 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-name*| *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]

no ip msdp [**vrf** *vrf-name*] **peer** {*peer-name*| *peer-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.

Release	Modification
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 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-address*| *peer-name*}[**list** *access-list-name*][**route-map** *map-name*][**rp-list**{*access-list-range*| *access-list-name*}][**rp-route-map** *route-map reference*]

no ip msdp[**vrf** *vrf-name*]**sa-filter out** {*peer-address*| *peer-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.

Release	Modification
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.
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-address*| *peer-name*}[*sa-limit*]

no ip msdp[**vrf** *vrf-name*]**sa-limit** {*peer-address*| *peer-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.

Release	Modification
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.

Command	Description
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-address*| *peer-name*}

no ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address*| *peer-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.

Release	Modification
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-address*| *peer-name*}

no ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address*| *peer-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 multicast boundary

To configure an administratively scoped IPv4 multicast boundary, use the **ip multicast boundary**command in interface configuration mode. 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 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 3.2S and Later Releases

no ip multicast boundary

Syntax Description

access-list	Number or name identifying an access control list (ACL) that controls the range of group addresses or (S, G) traffic affected by the boundary.
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
11.1	This command was introduced.

Release	Modification
12.0(22)S	The **filter-autorp** keyword was added.
12.1(12c)E	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.1(12c)E.
12.2(11)	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(11).
12.2(13)T	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	The **in** and **out** keywords 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.
Cisco IOS XE Release 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.

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.

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
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating in Protocol Independent Multicast (PIM).

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.

Release	Modification
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.
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 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-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.

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 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.
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.

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 pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration or virtual network interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

ip pim {**dense-mode** [**proxy-register** {**list** *access-list*| **route-map** *map-name*}]| **passive**| **sparse-mode**| **sparse-dense-mode**}

no ip pim {**dense-mode** [**proxy-register** {**list** *access-list*| **route-map** *map-name*}]| **passive**| **sparse-mode**| **sparse-dense-mode**}

Syntax Description

dense-mode	Enables dense mode of operation.
proxy-register	(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR.
list *access-list*	(Optional) Defines an extended access list number or name.
route-map *map-name*	(Optional) Defines a route map.
passive	Enables passive mode of operation.
sparse-mode	Enables sparse mode of operation.
sparse-dense-mode	Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.

Command Default

PIM is disabled on all interfaces.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
11.1	This command was modified. The **sparse-dense-mode**keyword was added.

Release	Modification
12.0S	This command was modified. The following keywords and arguments were added: • **proxy-register** • **list** *access-list* • **route-map** *map-name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **passive** keyword was added.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, passive mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets that it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface.

In Cisco IOS XE Release 3.2S and later releases, when PIM is enabled on an interface but the **ip multicast-routing** command has not been configured, a warning message, informing the user that the **ip multicast-routing** command is not configured and that multicast packets will not be forwarded, is no longer displayed.

Dense Mode

Initially, a dense mode interface forwards multicast packets until the router determines that there are group members or downstream routers, or until a prune message is received from a downstream router. Then, the dense mode interface periodically forwards multicast packets out the interface until the same conditions occur. Dense mode assumes that multicast group members are present. Dense mode routers never send a join message. They do send prune messages as soon as they determine they have no members or downstream PIM routers. A dense mode interface is subject to multicast flooding by default.

Dense Mode with Proxy Registering

For a router in a PIM sparse mode (PIM-SM) domain configured to operate in sparse mode or sparse-dense mode, the **ip pim dense-mode proxy-register** command must be configured on the interface leading toward the bordering dense mode region. This configuration will enable the router to register traffic from the dense mode region with the rendezvous point (RP) in the sparse mode domain.

Prior to Cisco IOS Release 12.0S, an RP needed to be running on the border router leading toward a dense mode region so that the RP could learn about traffic from sources in the dense mode region.

This command requires an extended access list or route map argument specifying which traffic the router needs to register with the RP. This command applies only to sources reachable through a PIM router. Cisco IOS software will always register traffic from remote sources if it arrives on a dense mode interface and if the Reverse Path Forwarding (RPF) neighbor leading toward the source is a Distance Vector Multicast Routing Protocol (DVMRP) but not a PIM router. This functionality has existed since Cisco IOS Release 10.0 and cannot be modified (restricted) with an access list or route map.

Passive Mode

An interface configured with passive mode does not pass or forward PIM control plane traffic; it passes or forwards only IGMP traffic. If passive mode is configured on an interface enabled for IP multicast, the router will not send PIM messages on the interface nor will it accept PIM messages from other routers on this interface. The router acts as the only PIM router on the network and works as the designated router (DR) and the designated forwarder (DF) for all Bidirectional PIM group ranges.

The **ip pim neighbor-filter** command has no effect and is superseded by the **ip pim passive** command when both commands are configured on the same interface.

Do not use the **ip pim passive** command on LANs that have more than one IP multicast router connected to them, because all routers with this command become DR and DF, resulting in duplicate traffic (PIM-SM, PIM-DM, PIM-SSM) or looping traffic (Bidir-PIM). To limit PIM messages to and from valid routers on LANs with more than one router, use the **ip pim neighbor-filter** command

Sparse Mode

A sparse mode interface is used for multicast forwarding only if a join message is received from a downstream router or if group members are directly connected to the interface. Sparse mode assumes that no other multicast group members are present. When sparse mode routers want to join the shared path, they periodically send join messages toward the RP. When sparse mode routers want to join the source path, they periodically send join messages toward the source; they also send periodic prune messages toward the RP to prune the shared path.

Sparse-Dense Mode

An alternative to choosing just dense mode or just sparse mode is to run PIM in a single region in sparse mode for some groups and dense mode for other groups.

In sparse-dense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is “sparse” if the router knows about an RP for that group.

When an interface is treated in dense mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- Any of the PIM neighbors on the interface have not pruned for the group.

When an interface is treated in sparse mode, it is populated in the outgoing interface list of the multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- A PIM neighbor on the interface has received an explicit join message.

Examples

The following example shows how to enable PIM-SM on tunnel interface 0 and set the address of the RP router to 226.0.0.8:

```
ip pim rp-address 226.0.0.8
interface tunnel 0
 ip pim sparse-mode
```

The following example shows how to enable PIM dense mode (PIM-DM) on Ethernet interface 1:

```
interface ethernet 1
 ip pim dense-mode
```

The following example shows how to enable PIM sparse-dense mode on Ethernet interface 1:

```
interface ethernet 1
 ip pim sparse-dense-mode
```

The following example shows how to register the multicast traffic for any source and any multicast group:

```
interface ethernet 0
 ip address 172.16.0.0 255.255.255.0
 description Ethernet interface toward the PIM sparse-mode domain
 ip pim sparse-dense-mode
!
interface ethernet 1
 ip address 172.44.81.5 255.255.255.0
 description Ethernet interface toward the PIM dense-mode region
 ip pim dense-mode proxy-register list 100
!
access-list 100 permit ip any any
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip pim neighbor-filter	Filters PIM messages.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
show ip pim interface	Displays information about interfaces configured for PIM.

ip pim autorp listener

To cause IP multicast traffic for the two Auto-RP groups 224.0.1.39 and 224.0.1.40 to be Protocol Independent Multicast (PIM) dense mode flooded across interfaces operating in PIM sparse mode, use the ip pim autorp listener command in global configuration mode. To disable this feature, use the **no** form of this command.

ip pim autorp listener

no ip pim autorp listener

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(7)	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

Use the **ip pim autorp listener** command with interfaces configured for PIM sparse mode operation in order to establish a network configuration where Auto-RP operates in PIM dense mode and multicast traffic can operate in sparse mode, bidirectional mode, or Source Specific Multicast (SSM) mode.

Examples

The following example enables IP multicast routing and the Auto-RP listener feature on a router. It also configures the router as a candidate RP for the multicast groups 239.254.2.0 through 239.254.2.255.

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
access-list 1 permit 239.254.2.0 0.0.0.255
```

ip pim dm-fallback

To enable Protocol Independent Multicast (PIM) dense mode (DM) fallback, use the **ip pim dm-fallback** command in global configuration mode. To prevent PIM dense mode fallback, use the **no** form of this command.

ip pim dm-fallback

no ip pim dm-fallback

Syntax Description

This command has no arguments or keywords.

Command Default

PIM dense mode fallback is enabled for all interfaces on the router that are configured with either the **ip pim dense-mode**or **ip pim sparse-dense-mode** commands.

Command Modes

Global configuration (config)

Command History

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

If you use IP multicast in mission-critical networks, you should avoid the use of PIM-DM (dense mode).

Dense mode fallback describes the event of the PIM mode changing (falling back) from sparse mode (which requires an RP) to dense mode (which does not use an RP). Dense mode fallback occurs when RP information is lost.

If all interfaces are configured with the **ip pim sparse-mode** command, there is no dense mode fallback because dense mode groups cannot be created over interfaces configured for sparse mode.

Use the **no ip pim dm-fallback** command to disable PIM-DM flooding on sparse-dense interfaces.

Cause and Effect of Dense Mode Fallback

PIM determines whether a multicast group operates in PIM-DM or PIM-SM mode based solely on the existence of RP information in the group-to-RP mapping cache. If Auto-RP is configured or a bootstrap router (BSR) is used to distribute RP information, there is a risk that RP information can be lost if all RPs, Auto-RP, or the

BSR for a group fails due to network congestion. This failure can lead to the network either partially or fully falling back into PIM-DM.

If a network falls back into PIM-DM and AutoRP or BSR is being used, dense mode flooding will occur. Routers that lose RP information will fallback into dense mode and any new states that must be created for the failed group will be created in dense mode.

Effects of Preventing Dense Mode Fallback

Prior to the introduction of PIM-DM fallback prevention, all multicast groups without a group-to-RP mapping would be treated as dense mode.

With the introduction of PIM-DM fallback prevention, the PIM-DM fallback behavior has been changed to prevent dense mode flooding. By default, if all of the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command), there is no need to configure the **no ip pim dm-fallback** command (that is, the PIM-DM fallback behavior is enabled by default). If any interfaces are not configured using the **ip pim sparse-mode**command (for example, using the **ip pim sparse-dense-mode** command), then the PIM-DM fallback behavior can be explicit disabled using the **no ip pim dm-fallback**command.

When the **no ip pim dm-fallback** command is configured or when **ip pim sparse-mode** is configured on all interfaces, any existing groups running in sparse mode will continue to operate in sparse mode but will use an RP address set to 0.0.0.0. Multicast entries with an RP address set to 0.0.0.0 will exhibit the following behavior:

- Existing (S, G) states will be maintained.
- No PIM Join or Prune messages for (*, G) or (S, G, RPbit) are sent.
- Received (*, G) or (S, G, RPbit) Joins or Prune messages are ignored.
- No registers are sent and traffic at the first hop is dropped.
- Received registers are answered with register stop.
- Asserts are unchanged.
- The (*, G) outgoing interface list (olist) is maintained only for the Internet Group Management Protocol (IGMP) state.
- Multicast Source Discovery Protocol (MSDP) source active (SA) messages for RP 0.0.0.0 groups are still accepted and forwarded.

Examples

The following example shows how to disable PIM-DM fallback:

```
no ip pim dm-fallback
```

Related Commands

Command	Description
ip pim dense-mode	Enables PIM dense mode on the interface.
ip pim sparse-dense-mode	Enables PIM to operate in sparse or dense mode, depending on the group.

ip pim query-interval

To configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages, use the **ip pim query-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ip pim query-interval *period* **[msec]**

no ip pim query-interval

Syntax Description

period	The number of seconds or milliseconds (ms) that can be configured for the PIM hello (query) interval. The range is from 1 to 65535.
msec	(Optional) Specifies that the interval configured for the *period* argument be interpreted in milliseconds. If the **msec** keyword is not used along with the *period* argument, the interval range is assumed to be in seconds.

Command Default

PIM hello (query) messages are sent every 30 seconds.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	The **msec** keyword was added.
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.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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 Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use this command to configure the frequency of PIM neighbor discovery messages. By default these messages are sent once every 30 seconds. In PIM Version 1 (PIMv1), these messages are referred to as PIM query messages; in PIM Version 2 (PIMv2), these messages are referred to as PIM hello messages. By default, routers run PIMv2 and send PIM hello messages. A router will change (auto-fallback) to PIMv1 and will send PIM query messages if it detects a neighboring router that only supports PIMv1. As soon as that neighboring PIMv1 router is removed from the network, the router will revert to PIMv2.

Note A router can be configured to exclusively use PIMv1 on an interface with the **ip pim version 1** command.

Note In PIM version 2, PIM hello messages also contain a variety of options that allow PIM routers on the network to learn about the capabilities of PIM neighbors. For more information about these capabilities, see the **show ip pim neighbor** command page.

PIM neighbor discovery messages are used to determine which router on a network is acting as the Designated Router (DR) for PIM sparse mode (PIM-SM) and Source Specific Multicast (SSM). The DR is responsible for joining PIM-SM and SSM groups receiving multicast traffic from sources requested by receivers (hosts). In addition, in PIM-SM, the DR is also responsible for registering local sources with the RP. If the DR fails, a backup router will become the DR and then forward traffic for local receivers and register local sources.

The *period* argument is used to specify the PIM hello (query) interval. The interval determines the frequency at which PIM hello (query) messages are sent.

Note When an interfaces enabled for PIM comes up, a PIM hello (query) message is sent immediately. In some cases, the initial PIM hello (query) message may be lost.If the first PIM hello (query) does not get sent when an interface initially comes up, another one will be sent 3 seconds later regardless of the PIM hello (query) interval to ensure that there are no initialization delays.

The configured PIM hello interval also determines the holdtime used by a PIM router. The Cisco IOS software calculates the holdtime as follows:

3 * the interval specified for the *period* argument

By default, PIM routers announce the holdtime in PIM hello (query) messages.If the holdtime expires and another router has not received another hello (query) message from this router, it will timeout the PIM neighbor. If the timed out router was the DR, the timeout will trigger DR election. By default, the DR-failover interval occurs after 90 seconds (after the default holdtime expires for a DR). To reduce DR-failover time in redundant networks, a lower value for the *period* argument can be configured on all routers. The minimum DR-failover time that can be configured (in seconds) is 3 seconds (when the *period* argument is set to 1 second). The DR-failover time can be reduced to less than 3 seconds if the **msecs** keyword is specified. When the **msecs** keyword is used with the **ip pim query-interval** command, the value specified for the *period* argument is interpreted as a value in milliseconds (instead of seconds). By enabling a router to send PIM hello messages more often, this functionality allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently

Note If IGMP Version 1 is being used on a network, then the DR is also the IGMP querier; if at least IGMP version 2 is being used, then the router with the lowest IP address becomes the IGMP querier.

Examples

The following example shows how to set the PIM hello interval to 45 seconds:

```
interface FastEthernet0/1
 ip pim query-interval 45
```

The following example shows how to set the PIM hello interval to 100 milliseconds:

```
interface FastEthernet0/1
 ip pim query-interval 100 msec
```

Related Commands

Command	Description
show ip pim neighbor	Displays information about PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages

ip pim register-rate-limit

To rate limit Protocol Independent Multicast sparse mode (PIM-SM) register packets based on either packets per second or bits per second, use the **ip pim register-rate-limit** command in global configuration mode. To disable this limit, use the **no** form of this command.

Cisco IOS Releases Prior to Releases 12.2(33)SRE and 15.0(1)M

ip pim [**vrf** *vrf-name*] **register-rate-limit** *packets-per-second*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Cisco IOS Releases 12.2(33)SRE, 15.0(1)M, and Cisco IOS XE Release 2.1, and Subsequent 12.2SR, 15.0 Mainline, T Releases, and Cisco IOS XE Releases

ip pim [**vrf** *vrf-name*] **register-rate-limit** *bits-per-second*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Syntax Description

vrf *vrf-name*	(Optional) Rate limits PIM-SM register packets associated with the Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name*argument.
packets-per-second	Maximum number of register packets sent per second by the router. The range is from 1 to 65535 seconds. By default, a maximum rate is not set.
bits-per-second	Maximum number of register bits sent per second. The range is from 8000 to 2000000000 bits. By default, a maximum rate is not set.

Command Default

No rate limit is set for PIM-SM register packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	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 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.

Release	Modification
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.
Cisco IOS XE Release 2.1	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of a bits per second on a per-RP basis.
15.0(1)M	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of bits per second on a per-RP basis.
12.2(33)SRE	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of bits per second on a per-RP basis.

Usage Guidelines

Use this command to rate limit the PIM-SM register packets based on either packets per second or bits per second. Enabling this command will limit the load on the DR and RP at the expense of dropping those register packets that exceed the set limit. Receivers may experience data packet loss within the first second in which register packets are sent from bursty sources.

Setting a value for the *packets-per-second* argument using the **ip pim register-rate-limit**command sets rate limiting on all PIM-SM registers.

Setting a value for the *bits-per-second* argument using the **ip pim register-rate-limit**command sets rate limiting on PIM-SM registers on a per-RP basis.

If the **ip pim**command is configured with the **dense-mode**and **proxy-register**keywords, you must set a limit on the maximum number of PIM-SM register packets sent because of the potentially large number of sources from the dense mode area that may send data into the sparse mode region (and thus need registering in the border router).

This command applies only to sparse mode (S, G) multicast routing entries.

Examples

The following example shows how to configure the **ip pim register-rate-limit**command with a maximum rate of two register packets per second:

```
ip pim register-rate-limit 2
```

The following examples shows how to configure the **ip pim register-rate-limit** command with a maximum rate of 8000 bits per second:

```
ip pim register-rate-limit 8000
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim rp-announce-filter

To filter incoming rendezvous point (RP) announcement messages sent from candidate RPs (C-RPs) to the RP mapping agent, use the **ip pim rp-announce-filter** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-announce-filter** {**group-list** *access-list*| **rp-list** *access-list* [**group-list** *access-list*]}

no ip pim [**vrf** *vrf-name*] **rp-announce-filter** {**group-list** *access-list*| **rp-list** *access-list* [**group-list** *access-list*]}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the filter be applied to incoming RP messages sent from C-RPs associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-list *access-list*	Specifies the number or name of a standard access list that defines the multicast groups to be permitted or denied from RP announcements sent by C-RPs to the RP mapping agent.
rp-list *access-list*	Specifies the number or name of a standard access list that defines the IP addresses of C-RPs whose RP announcements are to be permitted or denied by the RP mapping agent.

Command Default

All RP announcements are accepted by the RP mapping agent.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	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.

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

Usage Guidelines

Use the **ip pim rp-announce-filter** command to filter incoming Auto-RP announcement messages sent from C-RPs to RP mapping agents. This command should only be configured on RP mapping agents.

Auto-RP provides a means to distribute group-to-RP mappings within a multicast network without having to manually configure static RPs on every router. To accomplish this distribution, Auto-RP uses the following mechanisms:

- C-RPs send RP announcements to multicast group 224.0.1.39.
- RP mapping agents receive the RP announcements from C-RPs and determine which C-RP should be the RP for any given group (or groups) based on the highest IP address. RP mapping agents then distribute that information to all multicast routers by means of RP discovery messages, which are sent to the Auto-RP multicast group address 224.0.1.40.
- The sending of both RP announcements and RP discovery messages occurs every 60 seconds by default with a holdtime of 180 seconds. If no RP is found, each router then searches locally for a static RP mapping. If no static RP mapping is configured, the router defaults to dense mode.

The **ip pim rp-announce filter** command allows you to configure policies on an RP mapping agent that define the C-RPs whose RP announcements are to be filtered (ignored) by the mapping agent. You can use this command to configure the mapping agent to filter RP announcement messages from specific or unknown routers by permitting or denying specific C-RPs .You can also filter RP announcement messages from an candidate RP for specific group prefixes, thereby restricting that router to be the C-RP for only the ranges not filtered on the RP mapping agent.

Caution If you use more than one RP-mapping agent, you must configure the same filters on all mapping agents to avoid inconsistencies in Auto-RP operations.

Caution An improperly configured **ip pim rp-announce-filter**command may result in RP announcements being ignored. In addition, the **ip pim rp-announce-filter** command should only be configured on the mapping agent; if not, the command will fail because non-mapping agents do not listen to group 224.0.1.39 and do not know how to distribute the necessary group-to-RP mappings.

Use the **rp-list** keyword and *access-list* argument to specify the standard access list that defines the IP addresses of C-RPs whose RP announcements are to be permitted or denied on the RP mapping agent. Use the **group-list**keyword and *access-list* argument to specify the standard access list that defines the multicast groups to be permitted or denied from RP announcements sent by C-RPs to the RP mapping agent. RP announcment messages received that match the access list specified for **rp-list** keyword and access list specified for the **group-list** keyword are filtered by the RP mapping agent.

If a C-RP list is not specified (using the **rp-list** keyword and *access-list*argument), the command will permit all C-RPs. If a group list is not specified (using the **group-list** keyword and *access-list* argument), the command will deny all groups.

If no **ip pim rp-announce-filter** commands are configured, a router enabled to be an RP mapping agent (using the **ip pim send-rp-discovery** command) will accept all RP announcements for all groups from all C-RPs. Configure one or more **ip pim rp-announce-filter**commands on RP mapping agents to filter unwanted RP messages.

Examples

The following example shows how to configure the router to accept RP announcements from the C-RPs defined in access list 1 for the group range defined in access list 2:

```
ip pim rp-announce-filter rp-list 1 group-list 2
access-list 1 permit 10.0.0.1
access-list 1 permit 10.0.0.2
access-list 2 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim send-rp-discovery	Configures the router to be an RP mapping agent.

ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this router as an RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** {*interface-type interface-number*| *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] **[bidir]**

no ip pim [**vrf** *vrf-name*] **send-rp-announce** {*interface-type interface-number*| *ip-address*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and number that is used to define the RP address. No space is required between the values.
ip-address	IP address of the RP for the group. The IP address must be a directly connected address. If the command is configured with this argument, the RP-announce message will be sourced by the interface to which this IP address is connected (that is, the source address in the IP header of the RP-announce message is the IP address of that interface).
scope *ttl-value*	Specifies the time-to-live (TTL) value that limits the number of Auto-RP announcements.
group-list *access-list*	(Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Specifies the interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds.

bidir	(Optional) Indicates that the multicast groups specified by the *access-list*argument are to operate in bidirectional mode. If the command is configured without this keyword, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).

Command Default Auto-RP is disabled.*seconds*: 60

Command Modes Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(2)T	This command was modified. The following keywords and argument were added: • **interval** *seconds* • **bidir**
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.
12.4(5)	This command was modified. The *ip-address* argument was added.
12.3(17)	This command was modified. The *ip-address* argument was added.
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.
12.2(33)SRE	This command was modified. The *ip-address* argument was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
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

Enter this command on the router that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-RP mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address**command.

Examples

The following example shows how to configure the router to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as RP is the IP address associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as RP.

```
ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.

ip pim send-rp-discovery

To configure the router to be a rendezvous point (RP) mapping agent, use the **ip pim send-rp-discovery**command in global configuration mode. To deconfigure the router from functioning as the RP mapping agent, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]

no ip pim [**vrf** *vrf-name*] **send-rp-discovery**

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to be an RP mapping agent for the specified Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance.
interface-type interface-number	(Optional) Interface type and number that is to be used as the source address of the RP mapping agent.
scope *ttl-value*	Specifies the time-to-live (TTL) value for Auto-RP discovery messages. The range is from 1 to 255.
interval *seconds*	(Optional) Specifies the interval at which Auto-RP discovery messages are sent. The range is from 1 to 16383. **Note** By default, Auto-RP discovery messages are sent at an interval of 60 seconds or when the RP mapping agent detects changes.

Command Default

The router is not configured to be an RP mapping agent.

Command Modes

Global configuration

Command History

Release	Modification
11.1	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.

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.
12.4(8)	The **interval** keyword and *seconds* argument were added.
12.4(9)T	The **interval** keyword and *seconds* argument were added.
12.2(33)SRB	The **interval** keyword and *seconds* argument were added.
12.2(18)SXF11	The **interval** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip pim send-rp-discovery** command to configure the router to be an RP mapping agent. An RP mapping agent receives Auto-RP announcement messages, which it stores in its local group-to-RP mapping cache. The RP mapping agent uses the information contained in the Auto-RP announcement messages to elect the RP. The RP mapping agent elects the candidate RP with the highest IP address as the RP for a group range.

The required **scope** keyword and *ttl-value* argument are used to specify the TTL value in the IP header of Auto-RP discovery messages.

Note For the **scope** keyword and *ttl-value* argument, specify a TTL large enough to cover your Protocol Independent Multicast (PIM) domain.

The optional **interval** keyword and *seconds* argument are used to specify the interval at which Auto-RP discovery messages are sent. By default, Auto-RP discovery messages are sent at an interval of 60 seconds or when the RP mapping agent detects changes.

Note Lowering the interval at which Auto-RP discovery messages are sent from the default value of 60 seconds results in more frequent floodings of the group-to-RP mappings. In some network environments, the disadvantages of lowering the interval (more control packet overhead) may outweigh the advantages (more frequent group-to-RP mapping updates).

When Auto-RP is used, the following events occur:

1. The RP mapping agent listens for Auto-RP announcement messages sent by candidate RPs to the well-known group address CISCO-RP-ANNOUNCE (224.0.1.39).
2. The RP mapping agents stores the information learned from Auto-RP announcement messages in its local group-to-RP mapping cache.
3. The RP mapping agents elects the candidate RP with the highest IP address as the RP and announces the RP in the Auto-RP discovery messages that it sends out.
4. The Auto-RP discovery messages that the RP mapping agent sends to the well-known group CISCO-RP-DISCOVERY (224.0.1.40), which Cisco routers join by default, contains the elected RP learned from the RP mapping agent's group-to-RP mapping cache.

5 PIM designated routers listen for the Auto-RP discovery messages sent to 224.0.1.40 to learn the RP and store the information about the RP in their local group-to-RP mapping caches.

Use the **show ip pim rp** command with the **mapping** keyword to display all the group-to-RP mappings that the router has learned from Auto-RP.

Examples

The following example shows how to configure a router to be an RP mapping agent. In this example, the RP mapping agent is configured to use loopback 0 as the source address for Auto-RP messages. The Auto-RP discovery messages sent by the RP mapping agent are configured to be sent out at an interval of 50 seconds with a TTL of 20 hops.

```
ip pim send-rp-discovery loopback 0 scope 20 interval 50
```

Related Commands

Command	Description
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.

ip pim spt-threshold

To configure when a Protocol Independent Multicast (PIM) leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold**command in global configuration mode. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps*| **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps*| **infinity**} [**group-list** *access-list*]

Cisco IOS T-Train Release

ip pim [**vrf** *vrf-name*] **spt-threshold** {**0**| **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {**0**| **infinity**} [**group-list** *access-list*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
kbps	Traffic rate; valid values are from 0 to 4294967 kbps.
infinity	Causes all sources for the specified group to use the shared tree.
group-list *access-list*	(Optional) Specifies the groups to which the threshold applies. Must be an IP standard access list number or name. If the value is 0, the threshold applies to all groups.
0	Specifies to always switch to the source tree.

Command Default

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	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.

Release	Modification
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

If a source sends at a rate greater than or equal to traffic rate (the *kbps* value), a PIM join message is triggered toward the source to construct a source tree.

If the **infinity** keyword is specified, all sources for the specified group will use the shared tree. Specifying a **group-list** *access-list* indicates the groups to which the threshold applies.

If the traffic rate from the source drops below the threshold traffic rate, the leaf router will switch back to the shared tree and send a prune message toward the source.

Examples

The following example shows how to set a threshold of 4 kbps. If the traffic rate exceeds this threshold, the traffic to a group from a source causes the router to switch to the shortest path tree to that source.

```
Router# configure terminal
Router(config)# ip pim spt-threshold 4
```

Related Commands

Command	Description
ip pim bidir-neighbor-filter	Configures an ACL to specify which bidirectionally capable neighbors will participate in the designated forwarder election.

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **ssm** {**default**| **range** *access-list*}

no ip pim [**vrf** *vrf-name*] **ssm** {**default**| **range** *access-list*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
default	Defines the SSM range access list to 232/8.
range *access-list*	Specifies the standard IP access list number or name defining the SSM range.

Command Default

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)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

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

Examples

The following example shows how to configure SSM service for the IP address range defined by access list 4:

```
access-list 4 permit 224.2.151.141
ip pim ssm range 4
```

Related Commands

Command	Description
ip igmp v3lite	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
ip urd	Enables interception of TCP packets sent to the reserved URD port 659 on an interface and processing of URD channel subscription reports.

ip pim state-refresh disable

To disable the processing and forwarding of PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh disable**command in global configuration mode. To reenable the processing and forwarding of PIM dense mode state refresh control messages, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **state-refresh disable**

no ip pim [**vrf** *vrf-name*] **state-refresh disable**

Syntax Description

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

Command Default

The processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports the PIM dense mode state refresh feature.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)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

Configuring this command removes PIM dense mode state refresh information from PIM hello messages.

Examples

The following example shows how to disable the periodic forwarding of the PIM dense mode state refresh control message down a source-based IP multicast distribution tree:

```
ip pim state-refresh disable
```

Related Commands

Command	Description
ip pim state-refresh origination-interval	Configures the origination of and the interval for the PIM dense mode state refresh control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

ip pim state-refresh origination-interval

To configure the origination of and the interval for PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh origination-interval**command in interface configuration mode. To stop the origination of the PIM dense mode state refresh control message, use the **no** form of this command.

ip pim state-refresh origination-interval [*interval*]

no ip pim state-refresh origination-interval [*interval*]

Syntax Description

interval	(Optional) The number of seconds between PIM dense mode state refresh control messages. The default is 60 seconds. The available interval range is from 4 to 100 seconds.

Command Default

PIM dense mode state refresh control message origination is disabled. By default, all PIM routers that are running a Cisco IOS software release that supports PIM dense mode state refresh can process and forward PIM dense mode state refresh control messages.

Command Modes

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

Command History

Release	Modification
12.1(5)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.
15.1(1)S	This command was modified. This command can be now be configured on an interface that is not enabled for PIM dense mode.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Configure this command on the interfaces of the first hop, PIM dense mode routers that are directly connected to sources for PIM-DM multicast groups.

In Cisco IOS Release 15.1(1)S and later releases, this command can be configured on an interface on which PIM sparse mode is enabled.

In Cisco IOS Release 15.1(0)S and earlier releases, this command can be configured on an interface only if PIM dense mode state refresh is enabled. If you attempt to configure this command on an interface on which PIM sparse mode is enabled, the following warning message is displayed.

```
Warning: PIM State-Refresh cannot be configured on sparse interface
```

By default, the processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports PIM dense mode state refresh.

Examples

The following example configures the origination of the state refresh control message on Ethernet interface 0 of a PIM dense mode router with an interval of 80 seconds:

```
interface ethernet 0
 ip pim state-refresh origination-interval 80
```

Related Commands

Command	Description
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh feature control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

ip rgmp

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

ip rgmp

no ip rgmp

Syntax Description

This command has no arguments or keywords.

Command Default

RGMP is not enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

The following features must be enabled on your switch:

- IP multicast

- IGMP snooping

Examples

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

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

Related Commands

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

manager

To specify the interface that is to act as the Manager for Multicast Routing Monitor (MRM), and to specify the multicast group address the Test Receiver will listen to, use the **manager**command in MRM manager configuration mode. To remove the Manager or group address, use the **no** form of this command.

manager *interface-type interface-number* **group** *ip-address*

no manager *interface-type interface-number* **group** *ip-address*

Syntax Description

interface-type interface-number	Interface type and number of the Manager. The IP address associated with this interface is the source address of the Manager.
group *ip-address*	Specifies the IP multicast group address that the Test Receiver will listen to.

Command Default

There is no MRM Manager configured.

Command Modes

MRM manager configuration (config-mrm-manager)

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

This command identifies the interface that acts as the Manager, and therefore is required in order to run MRM.

Examples

The following example shows how to configure Ethernet interface 0 as the Manager and the Test Receiver to listen to multicast group 239.1.1.1:

```
ip mrm manager test1
 manager ethernet 0 group 239.1.1.1
```

Related Commands

Command	Description
beacon (multicast routing monitor)	Changes the frequency, duration, or scope of beacon messages that the Manager sends to Test Senders and Test Receivers during an MRM test.
ip mrm accept-manager	Configures a Test Sender or Test Receiver to accept requests only from Managers that pass an access list.
show ip mrm manager	Displays test information for MRM.