ip pgm host through ip pim version

ip pgm host

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To enable Pragmatic General Multicast (PGM) Host, use the **ip pgm host** command in global configuration mode. To disable PGM Host and close all open PGM Host traffic sessions, use the **no** form of this command.

ip pgm host [**source-interface** *interface-type interface-number*| *connection-parameter*]

no ip pgm host

Syntax Description

source-interface *interface-type interface-number*	(Optional) Specifies the interface type and number on which to run PGM Host.
connection-parameter	(Optional) Configures advanced PGM Host connection parameters. The optional configuration parameters should be configured only by experts in PGM technology. See the table below for a comprehensive list of the optional connection parameters and their definitions.

Command Default PGM Host is not enabled.

Command Modes Global configuration

Command History

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

Usage Guidelines Using the **ip pgm host** command without a keyword or an argument enables PGM Host on the router and configures the router to source PGM packets through a virtual host interface.

Specifying a physical or logical interface type (for example, an Ethernet, serial, or loopback interface) with the **ip pgm host source-interface** command configures the router to source PGM packets out of the physical or logical interface.

> **Note** You must first enable PGM Host globally on the router using the **ip pgm host** command before sourcing PGM packets out of a physical or logical interface using the **ip pgm host source-interface** command.

Sourcing PGM packets through a virtual host interface enables the router to send and receive PGM packets through any router interface. The virtual host interface also serves as the interface to the multicast applications that reside at the PGM network layer.

Sourcing IP multicast traffic out a specific physical or logical interface configures the router to send PGM packets out that interface only and to receive packets on any router interface.

When both PGM Host and Router Assist are enabled on the router, the router can process received PGM packets as a virtual PGM Host, originate PGM packets and serve as its own first hop PGM network element, and forward received PGM packets. Refer to the "Configuring PGM Host and Router Assist" chapter of the *Cisco IOS IP Configuration Guide* for more information about PGM Router Assist.

The table below lists the available parameters for the *connection-parameter* argument. The parameters should be configured only by experts in PGM technology. Use the **no ip pgm host** *connection-parameter* command to return a parameter to its default value.

Table 1: ip pgm host Connection Parameters

Parameter	Definition
ihb-max *milliseconds*	(Optional) Sets the source path message (SPM) interheartbeat timer maximum. The default is 10000 milliseconds (ms).
ihb-min *milliseconds*	(Optional) Sets the SPM interheartbeat timer minimum. The default is 1000 ms.
join *milliseconds*	(Optional) Sets the amount of time the PGM Host waits, when running in router mode, for client requests. The default is 0 ms.
nak-gen-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM negative acknowledgment (NAK) data packet. The default is 60000 ms.
nak-rb-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits before sending a PGM NAK data packet. The default is 500 ms.
nak-rdata-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a re-sent PGM NAK (NAK RDATA) data packet. The default is 2000 ms.

Parameter	Definition
nak-rpt-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM NAK confirmation (NAK NCF) data packet. The default is 2000 ms.
ncf-max *packets-per-second*	(Optional) Sets the maximum number of PGM NAK confirmation data packets (NAK NCFs) the PGM Host sends per second. The default is infinite.
rx-buffer-mgmt {**full**| **minimum**}	(Optional) Sets the type of receive data buffers (full or minimum) for the PGM Host. The default is minimum.
spm-ambient-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM source path message (SPM) ambient data packet. The default is 6000 ms.
spm-rpt-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM SPM repeat data packet. The default is 3000 ms.
stream-type {**apdu** | **byte**}	(Optional) Sets the data stream type (apdu or byte) for the PGM Host. The default is apdu.
tpdu-size *number*	(Optional) Sets the size of the source transport data unit (TPDU) for the PGM Host. The available range is 41 through 16384 bytes. The default is 1400 bytes.
ttl *number*	(Optional) Sets the time-to-live (TTL) value on the PGM Host for sent multicast data packets. The default is 255 hops. The TTL value for a packet is decremented by 1 as the packet passes through a router.
tx-buffer-mgmt {**keep** | **return**}	(Optional) Sets the type of transmit data buffers (keep or return) for the PGM Host. The default is return.
tx-adv-method {**data** | **time**}	(Optional) Sets the type of advanced transmit window method (data or time) for the PGM Host. The default is time.
txw-adv-secs *milliseconds*	(Optional) Sets the size of the advanced transmit window for the PGM Host. The default is 6000 ms.
txw-adv-timeout-max *milliseconds*	(Optional) Sets the time after which a transmit window will be advanced regardless of observed NAKs.
txw-rte *bytes-per-second*	(Optional) Sets the data transmit rate for the PGM Host. The default is 16384 bytes per second.

Parameter	Definition
txw-secs *milliseconds*	(Optional) Sets the data transmit window size for the PGM Host. The default is 30000 ms.
txw-timeout-max *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for data packets, even if the PGM Host receives PGM NAK data packets. The default is 3600000 ms.

Examples

The following example enables PGM Host (both the source and receiver part of the PGM network layer) globally on the router and configures the router to source PGM packets through a virtual host interface:

```
ip pgm host
```
The following example enables PGM Host globally on the router and configures the router to source PGM packets out of physical Ethernet interface 0/1:

```
ip pgm host
ip pgm host source-interface ethernet 0/1
```

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm router	Enables PGM Router Assist and thereby allows PGM to operate more efficiently on the router.
show ip pgm host defaults	Displays the default values for PGM Host traffic.
show ip pgm host sessions	Displays open PGM Host traffic sessions.
show ip pgm host traffic	Displays PGM Host traffic statistics.

ip pgm router

To enable Pragmatic General Multicast (PGM) Router Assist and thereby allow PGM to operate more efficiently on the router, use the **ip pgm router**command in interface configuration mode. To disable PGM Router Assist for the interface, use the **no** form of this command.

ip pgm router

no ip pgm router

Syntax Description

This command has no arguments or keywords.

Command Default

PGM Router Assist is disabled for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(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.

Usage Guidelines

This command is highly recommended for optimal deployment of PGM Reliable Transport Protocol on a host.

Examples

In the following example, PGM Router Assist is configured on Ethernet interfaces 0 and 1:

```
ip multicast-routing
interface ethernet 0
 ip pim sparse-dense-mode
 ip pgm router
interface ethernet 1
 ip pim sparse-dense-mode
 ip pgm router
```

Related Commands

Command	Description
clear ip pgm router	Clears PGM traffic statistics.

Cisco IOS IP Multicast Command Reference

Command	Description
ip pgm host	Enables PGM Host.
show ip pgm router	Displays PGM Reliable Transport Protocol state and statistics.

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 accept-register

To configure a candidate rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register**command in global configuration mode. To remove the PIM register filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*| **route-map** *map-name*}

no ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*| **route-map** *map-name*}

Syntax Description

vrf *vrf-name*	(Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
list *access-list*	Specifies an extended access list number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied.
route-map *map-name*	Specifies a route map that defines the (S, G) traffic in PIM register messages to be permitted or denied.

Command Default   No PIM register filters are configured.

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

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list or route map provided for the **ip pim accept-register** command should only filter on IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is desired, use the **ip multicast boundary** command instead.

Note
If the RP is also the first hop designated router (DR) for directly connected sources, PIM register packets will not be filtered using the **ip pim accept-register**command. For this case, use the **ip multicast boundary** command to filter the directly connected source traffic.

Examples

The following example shows how to permit register packets for source address 172.16.10.1 sending to the SSM group range (232.0.0.0/8). All other PIM register messages not matching the extended access list (ssm-range) are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first hop routers.

```
ip pim accept-register list ssm-range
ip access-list extended ssm-range
 permit ip 172.16.10.1 0.0.0.255 232.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped IPv4 multicast boundary.

ip pim accept-rp

To configure a router to accept join or prune messages destined for a specified rendezvous point (RP) and for a specific list of groups, use the **ip pim accept-rp**command in global configuration mode. To remove that check, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address*| **auto-rp**} [*access-list*]

no ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address*| **auto-rp**} [*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.
rp-address	RP address of the RP allowed to send join messages to groups in the range specified by the group access list.
auto-rp	Accepts join and register messages only for RPs that are in the Auto-RP cache.
access-list	(Optional) Access list number or name that defines which groups are subject to the check.

Command Default
The command is disabled, so all join messages and prune messages are processed.

Command Modes
Global configuration

Command History

Release	Modification
10.2	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

This command causes the router to accept only (*, G) join messages destined for the specified RP address. Additionally, the group address must be in the range specified by the access list.

When the *rp-address* argument is one of the addresses of the system, the system will be the RP only for the specified group range specified by the access list. When the group address is not in the group range, the RP will not accept join or register messages and will respond immediately to register messages with register-stop messages.

Examples

The following example shows how to configure the router to accept join or prune messages destined for the RP at address 172.17.1.1 for the multicast group 224.2.2.2:

```
ip pim accept-rp 172.17.1.1 3
access-list 3 permit 224.2.2.2
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip pim allow-rp

To enable the PIM Allow RP feature for all IP multicast-enabled interfaces in an IPv4 device, use the **ip pim allow-rp** command in the global configuration mode. To return to the default value, use the **no** form of this command.

ip pim allow-rp [**group-list** *access-list*| **rp-list** *access-list* [**group-list** *access-list*]]

no ip pim allow-rp

Syntax Description

group-list	(Optional)Specifies an access control list (ACL) for a group of allowed group ranges.
rp-list	(Optional)Specifies an ACL for allowed rendezvous-point (RP) addresses.
access-list	(Optional) Unique number or name of a standard ACL.

Command Default   PIM Allow RP is disabled.

Command Modes   Global configuration (config)

Command History

Release	**Modification**
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1).

Usage Guidelines   Use this command to enable the receiving device in an IP multicast network to accept a (*, G) Join from an unexpected (different) RP address.

Before enabling PIM Allow RP, you must first use the **ip pim rp-address** command to define an RP.

Examples
```
!
ip pim rp-address 192.0.2.3
ip pim allow-rp
!
ipv6 pim rp-address 20::1:1:3
ipv6 pim allow-rp
```

Related Commands

Command	Description
ip pim rp-address	Statically configures the address of a PIM RP for multicast groups.

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 bidir-enable

To enable bidirectional Protocol Independent Multicast (bidir-PIM), use the **ip pim bidir-enable**command in global configuration mode. To disable bidir-PIM, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bidir-enable**

no ip pim [**vrf** *vrf-name*] **bidir-enable**

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 command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2	This command was integrated into Cisco IOS Release 12.2.
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

Bidir-PIM is disabled by default to ensure complete backward compatibility when upgrading a router to Cisco IOS Release 12.0(18)ST or a later release.

When bidir-PIM is disabled, the router will behave similarly to a router without bidir-PIM support. The following conditions will apply:

- PIM hello messages sent by the router will not contain the bidirectional mode option.

- The router will not send designated forwarder (DF) election messages and will ignore DF election messages it receives.

- The **ip pim rp-address, ip pim send-rp-announce**, and **ip pim rp-candidate** global configuration commands will be treated as follows:

  - If these commands are configured when bidir-PIM is disabled, bidirectional mode will not be a configuration option.

  - If these commands are configured with the bidirectional mode option when bidir-PIM is enabled and then bidir-PIM is disabled, these commands will be removed from the command-line interface (CLI). In this situation, these commands must be configured again with the bidirectional mode option when bidir-PIM is reenabled.

- The **df** keyword for the **s how ip pim interface** user EXEC or privileged EXEC command and **debug ip pim** privileged EXEC command is not supported.

Examples

The following example shows how to configure a rendezvous point (RP) for both sparse mode and bidirectional mode groups: 224/8 and 227/8 are bidirectional groups, 226/8 is sparse mode, and 225/8 is dense mode. The RP must be configured to use different IP addresses for the sparse mode and bidirectional mode operations. Two loopback interfaces are used to allow this configuration. The addresses of these loopback interfaces must be routed throughout the PIM domain such that the other routers in the PIM domain can receive Auto-RP announcements and communicate with the RP.

```
ip multicast-routing
ip pim bidir-enable
!
interface loopback 0
description One Loopback adddress for this routers Bidir Mode RP function
ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface loopback 1
 description One Loopback adddress for this routers Sparse Mode RP function
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-dense-mode

ip pim send-rp-announce Loopback0 scope 10 group-list 45 bidir
ip pim send-rp-announce Loopback1 scope 10 group-list 46
ip pim send-rp-discovery scope 10

access-list 45 permit 224.0.0.0 0.255.255.255
access-list 45 permit 227.0.0.0 0.255.255.255
access-list 45 deny   225.0.0.0 0.255.255.255

access-list 46 permit 226.0.0.0 0.255.255.255
```

Related Commands

Command	Description
debug ip pim	Displays PIM packets received and sent, and to display PIM-related events.
ip pim rp-address	Configures the address of a PIM RP for a particular group.

Command	Description
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
ip pm send-rp-announce	Uses Auto-RP to configure for which groups the router is willing to act as RP.

ip pim bidir-neighbor-filter

To configure an access list (ACL) to specify which bidirectionally capable (bidir-capable) neighbors will participate in the designated forwarder (DF) election, use the **ip pim bidir-neighbor-filter**command in interface configuration mode. To allow all neighbors to participate in DF election, use the **no** form of this command.

ip pim bidir-neighbor-filter *acl-name*

no ip pim bidir-neighbor-filter *acl-name*

Syntax Description

acl-name	Specified ACL.

Command Default

All routers are considered to be bidirectional (bidir) capable.

Command Modes

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

Command History

Release	Modification
12.2(10)S	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)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.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Normally, DF election only occurs on those interfaces on which all Protocol Independent Multicast (PIM) neighbors are bidir capable. To allow for a smoother transition from a sparse-mode only network to a hybrid bidir-/sparse-mode network, the **ip pim bidir-neighbor-filter**command enables you to specify what routers should be participating on the DF election, while still allowing all routers to participate in the sparse-mode domain.

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled in order for bidir to elect a DF. Because routers in a segment are not always bidir-enabled, a mechanism is necessary to allow these routers to elect a DF from those routers on a segment that are bidir-enabled.

Multicast boundaries on the nonbidir routers are defined to prevent PIM messages and data for the bidir groups to leak in or out of the bidir subset cloud. Meanwhile, the bidir routers can elect a DF from among themselves even when there are nonbidir routers in the segment.

The ip pim bidir-neighbor-filter command allows the use of an ACL to specify which neighbors will participate in the DF election, allowing bidir deployment in the necessary routers without having to upgrade all of the routers in the segment.

Default behavior is that all routers are considered to be bidir-capable. Therefore, if one neighbor does not support bidir, the DF election will not occur.

When the ip pim bidir-neighbor-filter command is enabled, the routers that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election will not occur.

- If a denied neighbor does not support bidir, DF election still occurs among all other routers on the segment.

Examples   In the following example, the neighbor at address 10.4.0.3 is considered to be bidir-capable:

```
Router# show ip pim neighbor ethernet 3/3
PIM Neighbor Table
Neighbor          Interface             Uptime/Expires    Ver   DR
Address
Prio/Mode
10.4.0.4          Ethernet3/3           00:01:52/00:01:20 v2    1 / DR B
10.4.0.3          Ethernet3/3           00:01:52/00:01:20 v2    1 / B
Router# show access-lists 50
Standard IP access list 50
    10 permit 10.4.0.4 (3 matches)
    20 deny   10.4.0.3 (7 matches)
```
The **ip pim bidir-neighbor-filter 50** command sets conditions for DF election through use of ACL 50.

```
Router(config) interface ethernet 3/3
Router(config-if)# ip pim bidir-neighbor-filter 50
```
The following example shows the neighbor router at address 10.4.0.4 is now permitted to participate in DF election, and the neighbor router at address 10.4.0.3 is now denied access to DF election:

```
Router# show run interface ethernet 3/3
Building configuration...
Current configuration :210 bytes
!
interface Ethernet3/3
 ip address 10.4.0.2 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip pim bidir-neighbor-filter 50
 ip pim sparse-dense-mode
 no ip route-cache cef
 no ip route-cache
 duplex half
 end
Router# show ip pim neighbor ethernet 3/3
PIM Neighbor Table
Neighbor          Interface             Uptime/Expires    Ver   DR
Address
Prio/Mode
10.4.0.4          Ethernet3/3           00:04:03/00:01:39 v2    1 / DR B
10.4.0.3          Ethernet3/3           00:04:03/00:01:38 v2    1 /
```

ip pim bidir-offer-interval

To configure the Protocol Independent Multicast (PIM) bidirectionally capable designated forwarder (DF) election offer message interval time, use the **ip pim bidir-offer-interval**command in global configuration mode. To disable the message interval configuration, use the **no** form of this command.

ip pim bidir-offer-interval *seconds* **[msec]**

no ip pim bidir-offer-interval *seconds* **[msec]**

Syntax Description

seconds	Interval time, in seconds. The valid range is from 1 to 20000.
msec	(Optional) Specifies interval in milliseconds (ms).

Command Default

The default value for interval time is 100 ms.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following examples shows how to set the message interval time to 22 seconds:

```
Router# configure terminal
Router(config)# ip pim bidir-offer-interval 22
```

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 bidir-offer-limit	Configures the PIM bidirectionally capable number of unanswered offers before it changes as the DF.

ip pim bidir-offer-limit

To configure the Protocol Independent Multicast (PIM) bidirectionally capable number of unanswered offers before it changes as the designated forwarder (DF), use the **ip pim bidir-offer-limit**command in global configuration mode. To remove the limit, use the **no** form of this command.

ip pim bidir-offer-limit *number*

no ip pim bidir-offer-limit *number*

Syntax Description

number	Limit of unanswered offers. The valid range is 4 to 100.

Command Default   The default value is three unanswered offers.

Command Modes   Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples   The following examples shows how to set the unanswered offer limit to 75:

```
Router# configure terminal
Router(config)# ip pim bidir-offer-limit 75
```

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.

Command	Description
ip pim bidir-offer-interval	Configures the PIM bidirectionally capable DF election offer message interval time.

ip pim border

The **ip pim border** command is replaced by the **ip pim bsr-border**command. See the description of the **ip pim bsr-border** command for more information.

ip pim bsr-border

To prevent bootstrap router (BSR) messages from being sent or received through an interface, use the **ip pim bsr-border**command in interface configuration mode. To disable this configuration, use the **no** form of this command.

ip pim bsr-border

no ip pim bsr-border

Syntax Description   This command has no arguments or keywords.

Command Default   The command is disabled.

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

Command History

Release	Modification
11.3 T	The **ip pim border** command was introduced.
12.0(8)	The **ip pim border** command was replaced by the **ip pim bsr-border** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines   When this command is configured on an interface, no Protocol Independent Multicast (PIM) Version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Note   This command does not set up multicast boundaries. It sets up only a PIM domain BSR message border.

Examples

The following example configures the interface to be the PIM domain border:

```
interface ethernet 1
ip pim bsr-border
```

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped boundary.
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.

ip pim bsr-candidate

To configure a router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate**command in global configuration mode. To remove this router as a candidate BSR, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]

no ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to announce its candidacy as a BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-type interface-number	Interface type and number on this router from which the BSR address is derived. This address is sent in BSR messages. **Note** This interface must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate BSRs. This implementation predates RFC 5059, which specifies that 64 be used as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from RFC 5059. To comply with the default priority value specified in the RFC, you must explicitly set the priority value to 64.

Command Default The router is not configured to announce itself as a candidate BSR.

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 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.

Usage Guidelines This command configures the router to send BSR messages to all its PIM neighbors, with the address of the designated interface as the BSR address.

Note The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command should be configured on backbone routers that have good connectivity to all parts of the PIM domain.

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) routers unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so no preexisting IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each router that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Note Cisco routers always accept and process BSR messages. There is no command to disable this function.

Cisco routers perform the following steps to determine which C-RP is used for a group:

1 A longest match lookup is performed on the group prefix that is announced by the BSR C-RPs.

2 If more than one BSR-learned C-RP are found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate**command) is preferred.

3 If more than one BSR-learned C-RP have the same priority, the BSR hash function is used to select the RP for a group.

4 If more than one BSR-learned C-RP return the same hash value derived from the BSR hash function., the BSR C-RP with the highest IP address is preferred.

Examples

The following example shows how to configure the IP address of the router on Gigabit Ethernet interface 0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
ip pim bsr-candidate Gigabit Ethernet 0/0 0 192
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim rp-candidate	Configures the router to advertise itself to the BSR as a PIMv2 C-RP.
show ip pim bsr-router	Displays information about a BSR.

ip pim bsr-candidate loopback

To configure a boot strap router (BSR) loopback interface for filtering C-RP advertisements, use the **ip pim bsr-candidate loopback**command in global configuration mode. To remove the filter, use the **no** form of this command.

ip pim bsr-candidate loopback[*interface-number*] [*hash-mask-length*] [*priority*] [**accept-rp-candidate** [*acl-number*| *acl-name*]]

no ip pim bsr-candidate loopback

Syntax Description

interface-number	Loopback interface number on this router. This address is sent in BSR messages. The range is from 1 to 2147483647.
hash-mask-length	(Optional) Length of a mask, in bits, that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The range is 0 to 32. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred.
accept-rp-candidate	(Optional) Specifies that the C-RP candidate is to be filtered.
acl-number	(Optional) Number of access control list (ACL) to be used to filter C-RP advertisements. The range is 100 to 199 for standard ACL numbers and 2000 to 2699 for extended ACLs.
acl-name	(Optional) Name of ACL to be used to filter C-RP advertisements.

Command Default   The router is not configured to announce itself as a loopback candidate BSR.

Command Modes   Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.

Usage Guidelines   Use this command to filter BSR C-RP advertisements at the BSR using an ACL.

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command should be configured on backbone routers that have good connectivity to all parts of the PIM domain.

Examples   The following example shows how to configure the IP address of the router on an interface to be a BSR C-RP:

```
ip pim bsr-candidate loopback 1 accept-rp-candidate 101
access-list 101 permit pim host 192.168.255.101 any log
access-list 101 deny pim any any log
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim rp-candidate	Configures the router to advertise itself to the BSR as a PIMv2 C-RP.
show ip pim bsr-router	Displays information about a BSR.

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 dr-priority

To set the priority for which a router is elected as the designated router (DR), use the **ip pim dr-priority**command in interface configuration mode. To disable this function, use the **no** form of this command.

ip pim dr-priority *priority-value*

no ip pim dr-priority *priority-value*

Syntax Description

priority-value	Value in the range from 0 to 4294967294 used to determine the priority of the router to be selected as the DR.

Command Default

The command is disabled.

Command Modes

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

Command History

Release	Modification
12.1(2)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When a DR is a candidate for election, the following conditions apply:

- The router with the highest priority value configured on an interface will be elected as the DR. If this priority value is the same on multiple routers, then the router with the highest IP address configured on an interface will be elected as the DR.

- If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers with this priority status, then the router with the highest IP address configured on an interface will be elected as the DR.

Examples

The following example sets the DR priority value of the Ethernet0 interface to 200:

```
interface Ethernet0
  ip address 10.0.1.2 255.255.255.0
  ip pim dr-priority 200
```

ip pim log-neighbor-changes

To log the Protocol Independent Multicast (PIM) neighboring up or down status and the designated router changes, use the **ip pim log-neighbor-changes**command in global configuration mode. To disable the configured parameters, use the **no** form of this command.

ip pim log-neighbor-changes

no ip pim log-neighbor-changes

Syntax Description   This command has no arguments or keywords.

Command Default   The PIM status changes are logged in.

Command Modes   Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines   This command enables syslog messages that help to generate a list of neighbor state changes.

Examples   The following examples shows how to disable the logging of the neighboring changes:

```
Router# configure terminal
Router(config)# no
 ip pim log-neighbor-changes
```

Related Commands

Command	Description
ip pim dr-priority	Sets the priority for which a router is elected as the designated router.

ip pim maximum group-mappings

To configure the maximum number of number of group to active rendezvous points (RPs) mappings that can be created for auto-RP or BSR, use the **ip pim maximum group-mappings** command in global configuration mode. To return to the default, use the **no** form of this command.

ip pim maximum group-mappings {**autorp** | **bsr**} *max-mappings*

no ip pim maximum group-mappings { **autorp** | **bsr**}

Syntax Description

autorp	Specifies that PIM group mappings are learned from auto-RP.
bsr	Specifies that PIM group mappings are learned from BSR.
max-mappings	Maximum number of PIM group mappings. The range is from 1 to 10000.

Command Default   No limit is configured for PIM group mappings.

Command Modes   Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.

Usage Guidelines   Use this command to limit the number of group-to-RP mappings that can be created. When the specified maximum number of mappings is reached, existing mappings are updated but new mappings cannot be created.

Use the **show ip pim rp mapping** command to display the count and limit for mappings when this command is configured and there are mappings created.

Examples
```
Router(config)# ip pim maximum group-mappings autorp 5
Router(config)# ip pim maximum group-mappings bsr 5
Router (config)# exit
Router# show running-config | inc max
ip pim maximum group-mappings autorp 5
ip pim maximum group-mappings bsr 5
```

Related Commands

Command	Description
show ip pim rp mapping	Displays the mappings for the PIM group to the active rendezvous points.

ip pim minimum-vc-rate

To configure the minimum traffic rate to keep virtual circuits (VCs) from being idled, use the **ip pim minimum-vc-rate**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip pim minimum-vc-rate *pps*

no ip pim minimum-vc-rate

Syntax Description

pps	Rate, in packets per second, below which a VC is eligible for idling. The default value is 0, which means all VCs are eligible for idling. The range is from 0 to 4294967295.

Command Default

The default rate is 0 pps, which indicates all VCs are eligible for idling.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command applies to an ATM interface only and also requires IP Protocol Independent Multicast sparse mode (PIM-SM).

An idling policy uses the **ip pim vc-count** *number* command to limit the number of VCs created by PIM. When the router stays at or below this number, no idling policy is in effect. When the next VC to be opened will exceed the number, an idling policy is exercised. Any virtual circuits with a traffic rate lower than the **ip pim minimum-vc-rate** command are subject to the idling policy.

Examples

The following example configures a minimum rate of 2500 pps over a VC, below which the VC is eligible for idling:

```
ip pim minimum-vc-rate 2500
```

Related Commands

Command	Description
ip pim vc-count	Changes the maximum number of VCs that PIM can open.

ip pim multipoint-signalling

To enable Protocol Independent Multicast (PIM) to open ATM multipoint switched virtual circuits (VCs) for each multicast group that a receiver joins, use the **ip pim multipoint-signalling**command in interface configuration mode. To disable the feature, use the **no** form of this command.

ip pim multipoint-signalling

no ip pim multipoint-signalling

Syntax Description   This command has no arguments or keywords.

Command Default   The command is disabled. All multicast traffic goes to the static map multipoint VC as long as the **atm multipoint-signalling** command is configured.

Command Modes   Interface configuration

Command History

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

Usage Guidelines   This command is accepted only on an ATM interface. It allows optimal multicast trees to be built down to ATM switch granularity. This command can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

Examples   The following example enables PIM to open ATM multipoint switched VCs for each multicast group that is joined:

```
ip pim multipoint-signalling
```

Related Commands

Command	Description
atm multipoint-signalling	Enables point-to-multipoint signaling to the ATM switch.

Command	Description
ip pim minimum-vc-rate	Configures the minimum traffic rate to keep VCs from being idled.
ip pim vc-count	Changes the maximum number of VCs that PIM can open.
show ip pim vc	Displays ATM virtual circuit status information for multipoint VCs opened by PIM.

ip pim nbma-mode

To configure a multiaccess WAN interface to be in nonbroadcast multiaccess (NBMA) mode, use the **ip pim nbma-mode**command in interface configuration mode. To disable this function, use the **no** form of this command.

ip pim nbma-mode

no ip pim nbma-mode

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

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

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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 on Frame Relay, Switched Multimegabit Data Service (SMDS), or ATM only, especially when these media do not have native multicast available. Do not use this command on multicast-capable LANs such as Ethernet or FDDI.

When this command is configured, each Protocol Independent Multicast (PIM) join message is tracked in the outgoing interface list of a multicast routing table entry. Therefore, only PIM WAN neighbors that have joined for the group will get packets sent as data-link unicasts. This command should only be used when the **ip pim sparse-mode** command is configured on the interface. This command is not recommended for LANs that have natural multicast capabilities.

Examples

The following example configures an interface to be in NBMA mode:

```
ip pim nbma-mode
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim neighbor-filter

To prevent a router from participating in Protocol Independent Multicast (PIM) (for example, to configure stub multicast routing), use the **ip pim neighbor-filter**command in interface configuration mode. To remove the restriction, use the **no** form of this command.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

Syntax Description

access-list	Number or name of a standard IP access list that denies PIM packets from a source.

Command Default

The command is disabled.

Command Modes

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

Command History

Release	Modification
11.3	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.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Examples

The following example enables stub multicast routing on Router A, which has an outgoing interface with IP address 10.0.0.1. Router B is a central router with an incoming interface with address 10.0.0.2. Access list 1 filters PIM messages from the source (stub Router A).

Examples

```
ip multicast-routing
ip pim dense-mode
ip igmp helper-address 10.0.0.2
```

Examples

```
ip multicast-routing
 ip pim dense-mode : or ip pim sparse-mode
```

```
 ip pim neighbor-filter 1
access-list 1 deny 10.0.0.1
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip igmp helper-address	Causes the system to forward all IGMP host reports and leave messages received on the interface to the specified IP address.

ip pim passive

To configure an interface to operate in Protocol Independent Multicast (PIM) passive mode, use the **ip pim passive** command in interface configuration mode. To disable PIM passive mode operation on an interface, use the **no** form of this command.

ip pim passive

no ip pim passive

Syntax Description   This command has no arguments or keywords.

Command Default   PIM passive mode operation is disabled.

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

Command History

Release	Modification
12.2(37)SE	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines   If the **ip pim passive** command is configured on an interface enabled for IP multicast, the router will operate this interface in PIM passive mode, which means that the router will not send PIM messages on the interface nor will it accept PIM messages from other routers across this interface. The router will instead consider that it is the only PIM router on the network and thus act as the Designated Router (DR) and also as the Designated Forwarder (DF) for all bidirectional PIM (bidir-PIM) group ranges. Operations of the Interior Gateway Management Protocol (IGMP) are unaffected by this command.

Note   Do not use the **ip pim passive** command on LANs that have more than one multicast router connected to them because all routers with this command configured will consider themselves to be DR/DF, resulting in duplicate traffic (for PIM sparse mode [PIM-SM], PIM dense mode [PIM-DM], and Source Specific Multicast [PIM-SSM]) or even in looping traffic (for bidir-PIM). Instead, use the **ip pim neighbor-filter** command to limit PIM messages to and from valid routers on LANs with more than one router.

Note The **ip pim passive** and **ip pim neighbor-filter** commands can be used together on an interface. If both commands are configured, the **ip pim passive** command will take precedence over the **ip pim neighbor-filter** command.

Use the **show ip pim interface** command to confirm the mode that PIM interfaces are operating in.

Examples The following example shows how to configure an interface to operate in PIM passive mode. In this example, a stub router is configured to support multicast stub routing. VLAN interface 100 is configured to operate in PIM passive mode.

```
ip multicast-routing
!
interface Vlan100
  ip pim sparse-mode
  ip igmp helper-address 172.16.32.1
  ip pim passive
!
interface GigabitEthernet1/0
  ip pim sparse-mode
!
ip pim ssm default
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating in PIM (for example, to configure multicast stub routing).
show ip pim interface	Displays information about interfaces configured for PIM.

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 redundancy

To enable Protocol Independent Multicast (PIM) redundancy on an interface and bind the PIM designated router (DR) to an Hot Standby Redundancy Protocol (HSRP) group for HSRP aware PIM, use **ip pim redundancy** command in interface configuration mode. To return to the default, use the **no** form of this command.

ip pim redundancy *group* **dr-priority** *priority*

no ip pim redundancy *group*

Syntax Description

group	Unique name of a previously configured HSRP group.
	Note The HSRP group name is case sensitive.
dr-priority	Specifies a redundancy priority value for the active PIM DR.
priority	Redundancy priority value for the active PIM DR. The range is 0 to 4294967294. The actual range depends on the value of the PIM DR priority. The minimum value is 2.
	• Because the redundancy priority must be greater than the value of the PIM DR priority and the default value for PIM DR priority is 1, the valid minimum value is 2.

Command Default   PIM redundancy is disabled on the interface.

Command Modes   Interface configuration (config-if)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to enable PIM redundancy on an interface and assign a redundancy priority value to the PIM DR.

The redundancy priority for a PIM DR must be greater than the configured or default value (1) of the PIM DR priority (value used to elect a device as PIM DR) on any device for which the same HSRP group is enabled or the HSRP Active will fail to win the DR election. The value for PIM DR priority is configured by using the **ip pim dr-priority** command. The default value of PIM DR priority is 1.

Use the **standby ip** command in interface configuration mode to activate HSRP and define an HSRP group on an interface.

Because HSRP group names are case sensitive, the value of the *group* argument in the **ip pim redundancy** *group* command must match the value in the **standby ip name** configuration for the HSRP group.

If the value of the *group* argument in the **ip pim redundancy** *group* command is invalid, the command will be accepted but a debug message will be issued indicating that the specified HSRP group does not exist.

If the **standby ip name** command was not configured for the HSRP group to be specified, use the default name of the HSRP group for the *group* argument. The default name for an HSRP group is: **hsrp**-*interface*-*groupnumber*, as in hsrp-Et0/0-1, where the following applies:

- *interface*--A two-letter designator for the interface type plus the interface number (Et0/0 for Ethernet 0/0) of the interface on which the HSRP group is configured.

- *groupnumber*--The group number of the HSRP group that you previously configured using the **standby ip** command.

Note

We recommend that you always configure the **standby ip name** command when configuring an HSRP group to be used for HSRP aware PIM.

Examples

```
interface Ethernet 0/0
 ip address 10.0.0.2 255.255.255.0
 standby 1 ip 192.0.2.99
 standby 1 name HSRP1
 ip pim redundancy HSRP1 dr-priority 50
```

Related Commands

Command	Description
ip pim dr-priority	Sets the priority at which a device is elected as the designated router (DR) for PIM.
standby ip	Activates HSRP on an interface and configures an HSRP group.
standby ip name	Defines a name for an HSRP group.

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 register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP), use the **ip pim register-source**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **register-source** *interface-type interface-number*

no ip pim [**vrf** *vrf-name*] **register-source**

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 interface number that identify the IP source address of a register message.

Command Default

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command Modes

Global configuration

Command History

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

Usage Guidelines   This command is required only when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation may occur if the source address is filtered such that packets sent to it will not be forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address will fail to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures.

If no IP source address is configured or if the configured source address is not in service, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of the register message. Therefore, we recommend using a loopback interface with an IP address that is uniquely routed throughout the PIM-SM domain.

Examples   The following example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

ip pim rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] **[override] [bidir]**

no ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] **[override] [bidir]**

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the static group-to-RP mapping be associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rp-address	IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.
access-list	(Optional) Number or name of a standard access list that defines the multicast groups to be statically mapped to the RP. **Note** If no access list is defined, the RP will map to all multicast groups, 224/4.
override	(Optional) Specifies that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
bidir	(Optional) Specifies that the static group-to-RP mapping be applied to a bidir-PIM RP. If the command is configured without the **bidir** keyword, the groups will operate in sparse mode. **Note** The **bidir** keyword is available as an optional keyword only if bidir-PIM has been enabled (using the **ip pim bidir-enable** command).

Command Default   No PIM static group-to-RP mappings are configured.

Command Modes   Global configuration (config)

Command History

Release	Modification
10.2	This command was introduced.
11.1	The **override** keyword was added.
12.1(2)T	The **bidir** keyword was added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines   In the Cisco IOS implementation of PIM, each multicast group individually operates in one of the following modes: dense mode, sparse mode, or bidirectional mode. Groups in sparse mode (PIM-SM) or bidirectional mode (bidir-PIM) use RPs to connect sources and receivers. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

The Cisco IOS software learns the mode and RP addresses of multicast groups through the following three mechanisms: static group-to-RP mapping configurations, Auto-RP, and bootstrap router (BSR). By default, groups will operate in dense mode. No commands explicitly define groups to operate in dense mode.

Use the **ip pim rp-address** command to statically define the RP address for PIM-SM or bidir-PIM groups (an **ip pim rp-address** command configuration is referred to as a static group-to-RP mapping).

You can configure a single RP for more than one group using an access list. If no access list is specified, the static RP will map to all multicast groups, 224/4.

You can configure multiple RPs, but only one RP per group range.

If multiple **ip pim rp-address** commands are configured, the following rules apply:

- Highest RP IP address selected regardless of reachability: If a multicast group is matched by the access list of more than one configured **ip pim rp-address** command, then the RP for the group is determined by the RP with the highest RP address configured.

- One RP address per command: If multiple **ip pim rp-address** commands are configured, each static group-to-RP mapping must be configured with a unique RP address (if not, it will be overwritten).This restriction also means that only one RP address can be used to provide RP functions for either sparse

mode or bidirectional mode groups. If you want to configure static group-to-RP mappings for both bidirectional and sparse mode, the RP addresses must be unique for each mode.

- One access list per command: If multiple **ip pim rp-address** commands are configured, only one access list can be configured per static group-to-RP mapping. An access list cannot be reused with other static group-to-RP mappings configured on a router.

- For the Cisco Catalyst 6500 Series switch: Overlapping group ranges are not supported when they are configured for PIM-SM and bidir-PIM modes on a Cisco Catalyst 6500. Avoid overlapping group ranges when configuring both the PIM-SM and bidir-PIM modes in the same configuration. For more information, see the Cisco Catalyst 6500 configuration example below.

If dynamic and static group-to-RP mappings are used together, the following rule applies to a multicast group: Dynamic group-to-RP mappings take precedence over static group-to-RP mappings--unless the **override** keyword is used.

Examples

The following example shows how to set the PIM RP address to 192.168.0.1 for all multicast groups (224/4) and defines all groups to operate in sparse mode:

```
ip pim rp-address 192.168.0.1
```
The following example shows how to set the bidir-PIM RP address to 172.16.0.2 for the multicast range 239/8.

```
access list 10 239.0.0.0 0.255.255.255
ip pim rp-address 172.16.0.2 10 bidir
```
For the Cisco Catalyst 6500 Series switch: In the following example, 192.0.2.1 is configured for PIM-SM mode and the remaining groups in the 192.0.2.0/24 range are configured for bidir-PIM mode. In this configuration, the longest-match statement, deny 192.0.2.1, is not supported in the access control list (ACL) configuration because overlapping group ranges for multicast bidir-PIM and PIM-SM modes are not supported.

```
ip pim rp-address 10.0.0.1 SM_ACL override
ip pim rp-address 10.0.0.2 BIDIR_ACL override bidir

ip access-list standard BIDIR_ACL
 deny 192.0.2.1
 permit 192.0.2.0 0.0.0.255

ip access-list standard SM_ACL
 permit 192.0.2.1
```

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 rp-candidate

To configure a router to advertise itself to the bootstrap router (BSR) as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate**command in global configuration mode. To remove this router as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* **[bidir]** [**group-list** *access-list*] [**interval** *seconds*] [**priority** *value*]

no ip pim [**vrf** *vrf-name*] **rp-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-type interface-number	IP address associated with this interface type and number to be advertised as a C-RP address .
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 option, the groups specified will operate in PIM sparse mode.
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 it must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Specifies the C-RP advertisement interval, in seconds. The range is from 1 to 16383. The default value is 60.

priority *value*	(Optional) Specifies the priority of the C-RP. Range is from 0 to 255. The default priority value is 0. The BSR C-RP with the lowest priority value is preferred.
	Note The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

Command Default   The router is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes   Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.1(2)T	This command was modified. The **bidir** keyword was added.
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.

Usage Guidelines   Use this command to configure the router to send PIMv2 messages that advertise itself as a candidate RP to the BSR.

This command should be configured on backbone routers that have good connectivity to all parts of the PIM domain.

The IP address associated with the interface specified for the *interface-type* and *interface-number*arguments will be advertised as the C-RP address.

Note The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

If the optional **group-list** keyword and *access-list* argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.

Use this command with the optional **bidir** keyword when you want bidirectional forwarding and you are using the PIM Version 2 BSR mechanism to distribute group-to-RP mappings. Other options are as follows:

- If you are using Auto-RP to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim send-rp-announce** 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.

When the **interval** keyword is specified, the C-RP advertisement interval is set to a value specified by the *seconds* argument. The default interval is 60 seconds. Reducing this interval to a time of less than 60 seconds can reduce the time required to fail over to a secondary RP at the expense of generating more PIMv2 messages.

When the **priority** keyword is specified, the router will announce itself to be a C-RP with the priority specified for the *value*argument. For more information about the BSR selection process, see the **ip pim bsr-candidate** command page.

Examples The following example shows how to configure the router to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 0/0. That RP is responsible for the groups with the prefix 239.

```
ip pim rp-candidate Gigabit Ethernet 0/0 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-announce-filter	Filters incoming Auto-RP announcement messages coming from the RP.
ip pim send-rp-announce	Uses Auto-RP to configure for which groups the router is willing to act as RP.

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 snooping (global configuration)

To enable Protocol Independent Multicast (PIM) snooping globally, use the **ip pim snooping** command in global configuration mode. To disable PIM snooping globally, use the **no** form of this command.

ip pim snooping

no ip pim snooping

Syntax Description

This command has no arguments or keywords.

Command Default

PIM snooping is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	This command was introduced.
12.2(17d)SXB	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 2.
12.2(18)SXF2	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

Examples

This example shows how to enable PIM snooping globally:

```
ip pim snooping
```
This example shows how to disable PIM snooping globally:

```
no ip pim snooping
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping (interface configuration)

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

ip pim snooping

no ip pim snooping

Syntax Description   This command has no arguments or keywords.

Command Default   PIM snooping is disabled on an interface.

Command Modes   Interface configuration

Command History

Release	Modification
12.2(17a)SX	This command was introduced.
12.2(17d)SXB	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 2.
12.2(18)SXF2	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines   PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

You must enable PIM snooping globally before enabling PIM snooping on an interface. To enable PIM snooping globally, use the **ip pim snooping** command in global configuration mode. When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

You can enable PIM snooping on VLAN interfaces only.

Examples   This example shows how to enable PIM snooping on a VLAN interface:

```
interface vlan 101
 ip pim snooping
```
This example shows how to disable PIM snooping on a VLAN interface:

```
interface vlan 101
 no ip pim snooping
```

Related Commands

Command	Description
ip pim snooping (global configuration)	Enables PIM snooping globally.
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping dr-flood

To enable flooding of the packets to the designated router, use the **ip pim snooping dr-flood** command in global configuration mode. To disable the flooding of the packets to the designated router, use the **no** form of this command.

ip pim snooping dr-flood

no ip pim snooping dr-flood

Syntax Description   This command has no arguments or keywords.

Command Default   The flooding of packets to the designated router is enabled by default.

Command Modes   Global configuration

Command History

Release	Modification
12.2(18)SXF	This command was introduced.
12.2(18)SXF2	This command implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 2 or Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines   PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

Enter the **no ip pim snooping dr-flood** command only on switches that have no designated routers attached.

The designated router is programmed automatically in the (S,G) O-list.

Examples   The following example shows how to enable flooding of the packets to the designated router:

```
ip pim snooping dr-flood
```
The following example shows how to disable flooding of the packets to the designated router:

```
no ip pim snooping dr-flood
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping suppress sgr-prune

To enable suppression of SGR-prune packets to the designated router, use the **ip pim snooping suppress sgr-prune** command in global configuration mode. To disable the suppression of the packets to the designated router, use the **no** form of this command.

ip pim snooping suppress sgr-prune

no ip pim snooping suppress sgr-prune

Syntax Description   This command has no arguments or keywords.

Command Default   The suppression of packets to the designated router is disabled by default.

Command Modes   Global configuration mode

Command History

Release	Modification
12.2(18)ZY	This command was introduced.
12.2(18)SXF	This command was introduced.

Usage Guidelines   If a shared tree and SPT diverge in a VLAN on your switch router, and you have PIM snooping configured, then duplicate multicast packets may be delivered in your network. PIM snooping may stop the prune message sent by the receiver from reaching the upstream switch router in the shared tree, which causes more than one upstream switch router to forward the multicast traffic. This situation causes duplicate multicast packets to be delivered to the receivers. The sending of duplicate multicast packets only lasts a couple of seconds because the PIM-ASSERT mechanism is initiated and stops the extraneous flow. However, the cycle repeats itself when the next prune message is sent. To stop this situation from occurring, enter the **no ip pim snooping suppress sgr-prune** command.

Examples   The following example shows how to enable suppression of the SGR-prune packets to the designated router:

```
Router(config)# ip pim snooping suppress sgr-prune
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim sparse sg-expiry-timer

To adjust the (S, G) expiry timer interval for Protocol Independent Multicast sparse mode (PIM-SM) (S, G) multicast routes (mroutes), use the **ip pim sparse sg-expiry-timer** command in global configuration mode. To restore the default setting with respect to this command, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **sparse sg-expiry-timer** *seconds* [**sg-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **sparse sg-expiry-timer**

Syntax Description

vrf *vrf-name*	(Optional) Configures the expiry timer for PIM-SM (S, G) mroute entries associated with the Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the vrf-name argument.
seconds	Duration of the expiry timer interval, in seconds. The range is from 181 (3 minutes 1 second) to 57600 (16 hours).
sg-list *access-list*	(Optional) Specifies that the time value for the expiry timer be applied only to the (S, G) mroute entries that match the extended access list specified for the *access-list*argument.

Command Default

The expiry timer interval for PIM-SM (S, G) mroute entries is set to 180 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE5	This command was introduced.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4.
12.2(35)SE	This command was integrated into Cisco IOS Release 12.2(35)SE.
12.2(25)SEE2	This command was integrated into Cisco IOS Release 12.2(25)SEE2.
15.0(1)M	This command was integrated into a release before Cisco IOS Release 15.0(1)M

Usage Guidelines   Use the **ip pim sparse sg-expire-timer**command to adjust the expiry timer interval for PIM-SM (S, G) mroute entries to a time value greater than the default expiry timer interval of 180 seconds. This command can be used to lock down the shortest-path tree (SPT) for intermittent sources in PIM-SM network environments, such as sources in trading floor environments that sporadically send financial data streams to multicast groups during trading floor hours.

When a source stops sending traffic to a multicast group, the corresponding (S, G) mroute entry eventually times out and the (S, G) entry is removed. When the source resumes sending traffic to the group, the (S, G) entry is rebuilt. During the short time interval before the (S, G) entry is rebuilt, the traffic is forwarded on the (*, G) forwarding entry. There is a small window of time before the (S, G) entry is completely built in which packets may be dropped. The **ip pim sparse sg-expiry-timer** command can be used to maintain the (S, G) entry so that it will not be removed and the stream will not potentially suffer packet loss.

Note   The **ip pim sparse sg-expire-timer** command only applies to PIM-SM (S, G) mroute entries and, thus, does not apply to PIM-SM (*, G) mroute entries.

Examples   The following example shows how to adjust the expiry timer interval to 36000 seconds (10 hours) for PIM-SM (S, G) entries that match the extended access list named test_acl.

```
ip pim sparse sg-expiry-timer 36000 sg-list test_acl
!
ip access-list extended test-acl
 permit ip any host 234.1.1.1
```

Related Commands

Command	Description
ip pim spt-threshold	Configures when a PIM leaf router should join the shortest path source tree for the specified group.

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 pim v1-rp-reachability

To send Protocol Independent Multicast version 1 (PIMv1) rendezvous point (RP) reachability packets, use the **ip pim v1-rp-reachability**command in global configuration mode. To stop the packets, use the **no** form of this command.

ip pim v1-rp-reachability

no ip pim v1-rp-reachability

Syntax Description   This command has no arguments or keywords.

Command Default   The command is enabled by default.

Command Modes   Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples   The following example shows how to set the PIMV1 RP reachability packets:

```
Router# configure terminal
Router(config)# ip pim v1-rp-reachability
```

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 vc-count

To change the maximum number of virtual circuits (VCs) that Protocol Independent Multicast (PIM) can open, use the **ip pim vc-count** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip pim vc-count *number*

no ip pim vc-count

Syntax Description

number	Maximum number of VCs that PIM can open. The default is 200 VCs. The range is from 1 to 65535.

Command Default

200 VCs per ATM interface or subinterface

Command Modes

Interface configuration

Command History

Release	Modification
11.3	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.

Examples

The following example allows PIM to open a maximum of 250 VCs:

```
ip pim vc-count 250
```

Related Commands

Command	Description
ip pim minimum-vc-rate	Configures the minimum traffic rate to keep VCs from being idled.
ip pim multipoint-signalling	Enables PIM to open ATM multipoint switched VCs for each multicast group that a receiver joins.
ip pim	Enables PIM on an interface.

Command	Description
show ip pim vc	Displays ATM VCs status information for multipoint VCs opened by PIM.

ip pim version

To configure the Protocol Independent Multicast (PIM) version of the interface, use the **ip pim version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip pim version [**1**| **2**]

no ip pim version

Syntax Description

1	(Optional) Configures PIM Version 1.
2	(Optional) Configures PIM Version 2.

Command Default   Version 2

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

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines   An interface in Version 2 mode automatically downgrades to Version 1 mode if that interface has a PIM Version 1 neighbor. The interface returns to Version 2 mode after all Version 1 neighbors disappear (that is, they are shut down or upgraded).

Examples   The following example configures the interface to operate in PIM Version 1 mode:

```
interface ethernet 0
 ip address 10.0.0.0 255.0.0.0
 ip pim sparse-dense-mode
 ip pim version 1
```