

# 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

<b>source-interface</b> <i>interface-type</i> <i>interface-number</i>	(Optional) Specifies the interface type and number on which to run PGM Host.
<i>connection-parameter</i>	(Optional) Configures advanced PGM Host connection parameters. The optional configuration parameters should be configured only by experts in PGM technology. See <a href="#">Table 1</a> for a comprehensive list of the optional connection parameters and their definitions.

## Defaults

PGM Host is not enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.1(1)T	This command was introduced.

## 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.

[Table 1](#) 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
<b>ihb-max</b> <i>milliseconds</i>	(Optional) Sets the source path message (SPM) interheartbeat timer maximum. The default is 10000 milliseconds (ms).
<b>ihb-min</b> <i>milliseconds</i>	(Optional) Sets the SPM interheartbeat timer minimum. The default is 1000 ms.
<b>join</b> <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits, when running in router mode, for client requests. The default is 0 ms.
<b>nak-gen-ivl</b> <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM negative acknowledgment (NAK) data packet. The default is 60000 ms.
<b>nak-rb-ivl</b> <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits before sending a PGM NAK data packet. The default is 500 ms.
<b>nak-rdata-ivl</b> <i>milliseconds</i>	(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.
<b>nak-rpt-ivl</b> <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM NAK confirmation (NAK NCF) data packet. The default is 2000 ms.
<b>nfc-max</b> <i>packets-per-second</i>	(Optional) Sets the maximum number of PGM NAK confirmation data packets (NAK NCFs) the PGM Host sends per second. The default is infinite.
<b>rx-buffer-mgmt</b> {full   minimum }	(Optional) Sets the type of receive data buffers (full or minimum) for the PGM Host. The default is minimum.
<b>spm-ambient-ivl</b> <i>milliseconds</i>	(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.
<b>spm-rpt-ivl</b> <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM SPM repeat data packet. The default is 3000 ms.
<b>stream-type</b> {apdu   byte }	(Optional) Sets the data stream type (apdu or byte) for the PGM Host. The default is apdu.

**Table 1** *ip pgm host Connection Parameters (continued)*

Parameter	Definition
<b>tpdu-size</b> <i>number</i>	(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.
<b>ttl</b> <i>number</i>	(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.
<b>tx-buffer-mgmt</b> { <b>keep</b>   <b>return</b> }	(Optional) Sets the type of transmit data buffers (keep or return) for the PGM Host. The default is return.
<b>tx-adv-method</b> { <b>data</b>   <b>time</b> }	(Optional) Sets the type of advanced transmit window method (data or time) for the PGM Host. The default is time.
<b>txw-adv-secs</b> <i>milliseconds</i>	(Optional) Sets the size of the advanced transmit window for the PGM Host. The default is 6000 ms.
<b>txw-adv-timeout-max</b> <i>milliseconds</i>	(Optional) Sets the time after which a transmit window will be advanced regardless of observed NAKs.
<b>txw-rte</b> <i>bytes-per-second</i>	(Optional) Sets the data transmit rate for the PGM Host. The default is 16384 bytes per second.
<b>txw-secs</b> <i>milliseconds</i>	(Optional) Sets the data transmit window size for the PGM Host. The default is 30000 ms.
<b>txw-timeout-max</b> <i>milliseconds</i>	(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
<b>clear ip pgm host</b>	Resets PGM Host connections to their default values and clears traffic statistics.
<b>ip pgm router</b>	Enables PGM Router Assist and thereby allows PGM to operate more efficiently on the router.
<b>show ip pgm host defaults</b>	Displays the default values for PGM Host traffic.

Command	Description
<code>show ip pgm host sessions</code>	Displays open PGM Host traffic sessions.
<code>show ip pgm host traffic</code>	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.

**Defaults** PGM Router Assist is disabled for the interface.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

**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
	<b>clear ip pgm router</b>	Clears PGM traffic statistics.
	<b>ip pgm host</b>	Enables PGM Host.
	<b>show ip pgm router</b>	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 mode. To disable PIM on the interface, use the **no** form of this command.

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

```
no ip pim
```

## Syntax Description

<b>sparse-mode</b>	Enables sparse mode of operation.
<b>sparse-dense-mode</b>	Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.
<b>dense-mode</b>	Enables dense mode of operation.
<b>proxy-register</b>	(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.
<b>list</b> <i>access-list</i>	(Optional) Defines the extended access list number or name.
<b>route-map</b> <i>map-name</i>	(Optional) Defines the route map.

## Defaults

IP multicast routing is disabled on all interfaces.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.0	This command was introduced.
11.1	The <b>sparse-dense-mode</b> keyword was added.
12.0 S	The following keywords and arguments were added: <ul style="list-style-type: none"> <li>• <b>proxy-register</b></li> <li>• <b>list</b> <i>access-list</i></li> <li>• <b>route-map</b> <i>map-name</i></li> </ul>

## 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, 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 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.

### 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 12.0 S, 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.

### 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 towards the PIM sparse-mode domain
  ip pim sparse-dense-mode
!
interface ethernet 1
  ip address 192.44.81.5 255.255.255.0
  description Ethernet interface towards the PIM dens-mode region
  ip pim dense-mode proxy-register list 100
!
access-list 100 permit ip any any
```

**Related Commands**

Command	Description
<b>ip multicast-routing</b>	Enables IP multicast routing or multicast distributed switching.
<b>ip pim rp-address</b>	Configures the address of a PIM RP for a particular group.
<b>show ip pim interface</b>	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 disable this function, 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

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<b>list</b> <i>access-list</i>	Defines the extended access list number or name.
<b>route-map</b> <i>map-name</i>	Defines the route map.

## Defaults

The command is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## 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.

## Examples

The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP. These statements need to be configured only on the RP.

```
ip pim accept-register list no-ssm-range

ip access-list extended no-ssm-range
deny ip any 232.0.0.0 0.255.255.255
permit ip any any
```

# 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

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>rp-address</i>	RP address of the RP allowed to send join messages to groups in the range specified by the group access list.
<b>auto-rp</b>	Accepts join and register messages only for RPs that are in the Auto-RP cache.
<i>access-list</i>	(Optional) Access list number or name that defines which groups are subject to the check.

## Defaults

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 <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## 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 states that the router will 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
```

■ ip pim accept-rp

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>access-list (IP standard)</b>	Defines a standard IP access list.

# 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.

---

**Defaults** This command is disabled by default.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(7)	This command was introduced.

---

---

**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

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

## Defaults

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 <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## 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 **show 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 !Enable IP multicast routing
ip pim bidir-enable !Enable bidir-PIM
!
interface loopback 0
description One Loopback address 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 address 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
<b>debug ip pim</b>	Displays PIM packets received and sent, and to display PIM-related events.
<b>ip pim rp-address</b>	Configures the address of a PIM RP for a particular group.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
<b>ip pm send-rp-announce</b>	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*

<b>Syntax Description</b>	<i>acl-name</i>	Specified ACL.
---------------------------	-----------------	----------------

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

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(10)S	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

**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 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.

## Defaults

The command is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.3 T	The <b>ip pim border</b> command was introduced.
12.0(8)	The <b>ip pim border</b> command was replaced by the <b>ip pim bsr-border</b> command.

## 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
<b>ip multicast boundary</b>	Configures an administratively scoped boundary.
<b>ip pim bsr-candidate</b>	Configures the router to announce its candidacy as a BSR.

# ip pim bsr-candidate

To configure the 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 for being a bootstrap router, 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

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>interface-type</i> <i>interface-number</i>	Interface type and number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with Protocol Independent Multicast (PIM).
<i>hash-mask-length</i>	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups.
<i>priority</i>	(Optional) Priority of the candidate BSR. Integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

## Defaults

The command is disabled.  
*priority*: 0



### Note

The Cisco IOS implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. 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 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 Modes

Global configuration

## Command History

Release	Modification
11.3 T	This command was introduced.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

**Usage Guidelines**

This command causes the router to send bootstrap messages to all its PIM neighbors, with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, it caches the current address and forwards the bootstrap message. Otherwise, it drops the bootstrap message.

This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate BSR.

**Examples**

The following example shows how to configure the IP address of the router on Ethernet interface 0/0 to be a candidate BSR with priority of 192:

```
ip pim bsr-candidate ethernet 0/0 192
```

**Related Commands**

Command	Description
<b>ip pim border</b>	Configures the interface to be the PIM domain border.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
<b>ip pim send-rp-discovery</b>	Configures the router to be an RP-mapping agent.
<b>show ip pim bsr</b>	Displays the BSR information.
<b>show ip pim rp</b>	Displays active RPs that are cached with associated multicast routing entries.

# 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*

<b>Syntax Description</b>	<i>priority-value</i>	Value in the range from 0 to 4294967294 used to determine the priority of the router to be selected as the DR.
---------------------------	-----------------------	--

<b>Defaults</b>	The command is disabled.
-----------------	--------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(2)T	This command was introduced.

<b>Usage Guidelines</b>	<p>When a DR is a candidate for election, the following conditions apply:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
-------------------------	--

<b>Examples</b>	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 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

<i>pps</i>	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.
------------	---

## Defaults

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.

## 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, which is described in the section “Limit the Number of VCs” in the “Configuring IP Multicast Routing” chapter of the *Cisco IOS IP Configuration Guide*.

## 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
<b>ip pim vc-count</b>	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.

**Defaults** 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.

**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
	<b>atm multipoint-signalling</b>	Enables point-to-multipoint signaling to the ATM switch.
	<b>ip pim minimum-vc-rate</b>	Configures the minimum traffic rate to keep VCs from being idled.
	<b>ip pim vc-count</b>	Changes the maximum number of VCs that PIM can open.
	<b>show ip pim vc</b>	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.

---

**Defaults**

The command is disabled.

---

**Command Modes**

Interface configuration

---

**Command History**

Release	Modification
11.0	This command was introduced.

---

**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
<b>ip pim</b>	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*

<b>Syntax Description</b>	<i>access-list</i>	Number or name of a standard IP access list that denies PIM packets from a source.
---------------------------	--------------------	--

**Defaults** The command is disabled.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3	This command was introduced.

**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).

### Router A Configuration

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

### Router B Configuration

```
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
```

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

# ip pim query-interval

To configure the frequency of Protocol Independent Multicast (PIM) router query 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

<i>period</i>	The number of seconds or milliseconds (ms) that can be configured for the query interval: <ul style="list-style-type: none"> <li>The interval range, in seconds, is from 1 to 65535.</li> <li>The interval range, in milliseconds, is from 1 to 65535.</li> </ul>
<b>msec</b>	(Optional) Specifies the interval, in milliseconds, at which periodic PIM hello messages are sent. If the <b>msec</b> keyword is not used along with the <i>period</i> argument, the interval range is assumed to be in seconds.

## Defaults

This command is enabled by default.  
The PIM hello messages are sent every 30 seconds.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was updated with the <b>msec</b> keyword, which allows you to specify the interval between PIM hello messages in milliseconds.
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.

## Usage Guidelines

Routers configured for IP multicast send PIM hello messages to determine which router will be the designated router for each LAN segment (subnet). The designated router sends Internet Group Management Protocol (IGMP) host query messages to all hosts on the directly connected LAN. When operating in sparse mode, the designated router sends source registration messages to the rendezvous point (RP). The designated router is the router with the highest IP address.

## Examples

The following example changes the PIM hello interval to 45 seconds:

```
interface tunnel 0
 ip pim query-interval 45
```

The following example changes the PIM hello interval to 100 milliseconds:

```
interface Ethernet1/0
ip address 172.16.1.3 255.255.255.0
ip pim query-interval 100 msec
```

---

**Related Commands**

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

---

# ip pim register-rate-limit

To set a limit on the maximum number of Protocol Independent Multicast sparse mode (PIM-SM) register messages sent per second for each (S, G) routing entry, use the **ip pim register-rate-limit** command in global configuration mode. To disable this limit, use the **no** form of this command.

```
ip pim [vrf vrf-name] register-rate-limit rate
```

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

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	Specifies that the rate-limit for register messages be applied to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
<i>rate</i>	Maximum number of register messages sent per second by the router. The range is from 1 to 65535 messages-per-second.

## Command Default

No limit is set on the number of register messages sent per second.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
11.3T	This command was introduced.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> 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.
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 limit the number of register messages that the designated router (DR) will allow for each (S, G) entry. Enabling this command will limit the load on the DR and the rendezvous point (RP) at the expense of dropping those register messages that exceed the set limit. Receivers may experience data packet loss within the first second in which register messages are sent from bursty sources.

When the **ip pim** command is configured with the **dense-mode** and **proxy-register** keywords, the **ip pim register-rate-limit** command also should be configured 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). If the **ip pim register-rate-limit** command is not configured in this scenario, the Cisco IOS software will automatically apply a limit of two messages per second and the following warning will be raised:

```
Warning: PIM register rate-limit set to 2 messages per second
```

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 four register messages per second:

```
ip pim register-rate-limit 4
```

---

**Related Commands**

Command	Description
<b>ip pim</b>	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

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>interface-type</i> <i>interface-number</i>	Interface type and interface number that identify the IP source address of a register message.

## Defaults

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 <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## 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 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

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies that the address of a PIM RP be associated with the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified for the <i>vrf-name</i> argument.
<i>rp-address</i>	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.
<i>access-list</i>	(Optional) Number or name of an access list that defines for which multicast groups the RP should be used.
<b>override</b>	(Optional) Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by Auto-RP.
<b>bidir</b>	(Optional) Indicates that the multicast groups specified by the <i>access-list</i> argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in PIM sparse mode.

## Command Default

No PIM RPs are configured.

## Command Modes

Global configuration

## Command History

Release	Modification
10.2	This command was introduced.
11.1	The <b>override</b> keyword was added.
12.1(2)T	The <b>bidir</b> keyword was added.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

## 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 or bidirectional mode need to have the IP address of one router to operate as the RP for the group. 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 configuration, Auto-RP, and bootstrap router (BSR). Use the **ip pim rp-address** command to statically define the mode of operations and RP address for multicast groups that are to operate in sparse mode or bidirectional mode. By default, groups will operate in dense mode. No commands explicitly define groups to operate in dense mode.

You can configure the Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine for which groups the RP can be used. If no access list is configured, the RP is used for all groups. A PIM router can use multiple RPs, but only one per group.

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

- Highest RP IP address selection: If a group is matched by the access list of more than one **ip pim rp-address** command whose prefix masks are all the same lengths, then the mode and RP for the group are determined by the **ip pim rp-address** command with the highest RP address parameter.
- Static evaluation: The mode and RP selection for a group are static and do not depend on the reachability of the individual RPs. The router will not start using an RP with a lower IP address or a shorter prefix length match if the better RP is not reachable. Use Auto-RP, BSR, or Anycast-RP to configure redundancy.
- One IP address per command: An IP address can be used as a parameter for only one **ip pim rp-address** command. If an **ip pim rp-address** command is configured with an IP address parameter that was previously used to configure an older **ip pim rp-address** command, then this old command will be replaced with the newly configured command. This restriction also means that only one IP address can be used to provide RP functions for either sparse mode or bidirectional mode groups. Use different IP addresses of the same router to provide RP functions for both sparse mode and bidirectional mode from the same router.
- One access list per command: A specific access list can be used as a parameter for only one **ip pim rp-address** command. If an **ip pim rp-address** command is configured with an access list parameter that was previously used to configure an older **ip pim rp-address** command, then this old command will be replaced with the newly configured command.

Static definitions for the group mode and RP address of the **ip pim rp-address** command may be used together with dynamically learned group mode and RP address mapping through Auto-RP or BSR. The following rules apply to a multicast group:

- Group mode and RP address mappings learned through Auto-RP and BSR take precedence over mappings statically defined by the **ip pim rp-address** command without the **override** keyword. Commands with the **override** keyword take precedence over dynamically learned mappings.
- 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 using the PIM Version 2 bootstrap mechanism to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.

## Examples

The following example shows how to set the PIM RP address to 192.168.0.0 for all multicast groups and defines all groups to operate in sparse mode:

```
ip pim rp-address 192.168.0.0
```



### Note

The same RP cannot be used for both bidirectional and sparse mode groups.

The following example shows how to set the PIM RP address to 172.16.0.0 for the multicast group 225.2.2.2 only:

```
access list 1 225.2.2.2 0.0.0.0
 ip pim rp-address 172.16.0.0
```

**Related Commands**

Command	Description
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>ip pim rp-candidate</b>	Configures the router to advertise itself as a PIM Version 2 candidate RP to the bootstrap router.
<b>ip pim send-rp-announce</b>	Uses Auto-RP to configure for which groups the router is willing to act as RP.

# ip pim rp-announce-filter

To filter incoming Auto-RP announcement messages coming from the rendezvous point (RP), 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 rp-list access-list group-list access-list
```

```
no ip pim [vrf vrf-name] rp-announce-filter rp-list access-list group-list access-list
```

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<b>rp-list</b> <i>access-list</i>	Specifies the number or name of a standard access list of RP addresses that are allowable for the group ranges supplied in the <b>group-list</b> <i>access-list</i> combination.
<b>group-list</b> <i>access-list</i>	Specifies the number or name of a standard access list that describes the multicast groups the RPs serve.

## Defaults

All RP announcements are accepted.

## Command Modes

Global configuration

## Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## Usage Guidelines

Configure this command on the Protocol Independent Multicast (PIM) RP mapping agent. We recommend that if you use more than one RP mapping agent, make the filters among them consistent so that there are no conflicts in mapping state when the announcing agent goes down.

## Examples

The following example configures the router to accept RP announcements from RPs in access list 1 for group ranges described 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 224.0.0.0 192.168.255.255
```

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

# ip pim rp-candidate

To configure the router to advertise itself to the bootstrap router (BSR) as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this router as an RP candidate, 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	
<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>interface-type</i> <i>interface-number</i>	The IP address associated with this interface type and number is advertised as a candidate RP address.
<b>bidir</b>	(Optional) Indicates that the multicast groups specified by the <i>access-list</i> argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in PIM sparse mode.
<b>group-list</b> <i>access-list</i>	(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.
<b>interval</b> <i>seconds</i>	(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
<b>priority</b> <i>value</i>	(Optional) Indicates the RP priority value. The range is from 0 to 255. The default value is 0.

## Defaults

The command is disabled.  
*seconds*: 60  
*priority*: 0



## Note

The Cisco IOS implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. 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 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 Modes

Global configuration

## Command History

Release	Modification
11.3 T	This command was introduced.
12.1(2)T	The <b>bidir</b> keyword was added.

Release	Modification
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

### Usage Guidelines

This command causes the router to send a PIM Version 2 message advertising itself as a candidate RP to the BSR. The addresses allowed by the access list, together with the router identified by the type and number, constitute the RP and its range of addresses for which it is responsible.

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate RP.

Use this command with the **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 PIM Version 2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

When the **interval** keyword is specified, the candidate 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 PIM Version 2 messages.

### Examples

The following example shows how to configure the router to advertise itself as a candidate RP to the BSR in its PIM domain. Standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Ethernet interface 2. That RP is responsible for the groups with the prefix 239.

```
ip pim rp-candidate ethernet 2 group-list 4
 access-list 4 permit 239.0.0.0 0.255.255.255
```

### Related Commands

Command	Description
<b>ip pim bsr-candidate</b>	Configures the router to announce its candidacy as a BSR.
<b>ip pim rp-address</b>	Configures the address of a PIM RP for a particular group.
<b>ip pim rp-announce-filter</b>	Filters incoming Auto-RP announcement messages coming from the RP.
<b>ip pim send-rp-announce</b>	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	
<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>interface-type</i> <i>interface-number</i>	Interface type and number that is used to define the RP address. No space is required between the values.
<i>ip-address</i>	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).
<b>scope</b> <i>ttl-value</i>	Specifies the time-to-live (TTL) value that limits the number of Auto-RP announcements.
<b>group-list</b> <i>access-list</i>	(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.
<b>interval</b> <i>seconds</i>	(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.
<b>bidir</b>	(Optional) Indicates that the multicast groups specified by the <i>access-list</i> 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).

**Defaults** Auto-RP is disabled.  
*seconds*: 60

**Command Modes** Global configuration

Command History	Release	Modification
	11.1	This command was introduced.
	12.1(2)T	The following keywords and argument were added: <ul style="list-style-type: none"> <li><b>interval</b> <i>seconds</i></li> <li><b>bidir</b></li> </ul>
	12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
	12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
	12.3(17)	The <i>ip-address</i> argument was added.
	12.4(5)	The <i>ip-address</i> argument was added.
	12.4(4)T	The <i>ip-address</i> argument was added.

### 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 sends 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
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>ip pim rp-address</b>	Configures the address of a PIM RP for a particular group.
<b>ip pim rp-candidate</b>	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 restore the default value, use the **no** form of this command.

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

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

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number that is used to define the RP mapping agent address.
<b>scope</b> <i>ttl-value</i>	Specifies the time-to-live (TTL) value in the IP header that keeps the discovery messages within this number of hops.

## Defaults

The router is not an RP mapping agent.

## Command Modes

Global configuration

## Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## Usage Guidelines

Configure this command on the router designated as an RP mapping agent. Specify a TTL large enough to cover your Protocol Independent Multicast (PIM) domain.

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

1. The RP mapping agent listens on well-known group address CISCO-RP-ANNOUNCE (224.0.1.39), which candidate RPs send to.
2. The RP mapping agent sends RP-to-group mappings in an Auto-RP discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). The TTL value limits how many hops the message can take.
3. PIM designated routers listen to this group and use the RPs they learn about from the discovery message.

## Examples

The following example limits Auto-RP RP discovery messages to 20 hops:

```
ip pim send-rp-discovery scope 20
```

# 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 {kpbs | infinity} [group-list access-list]
```

```
no ip pim [vrf vrf-name] spt-threshold
```

## Syntax Description

<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.
<i>kpbs</i>	Traffic rate (in kbps).
<b>infinity</b>	Causes all sources for the specified group to use the shared tree.
<b>group-list access-list</b>	(Optional) Indicates which groups the threshold applies to. Must be an IP standard access list number or name. If the value is 0 or is omitted, the threshold applies to all groups.

## Defaults

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

## Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## Usage Guidelines

If a source sends at a rate greater than or equal to traffic rate (the *kpbs* 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 sets a threshold of 4 kbps, above which traffic to a group from a source will cause the router to switch to the shortest path tree to that source:

```
ip pim spt-threshold 4
```

# 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
```

## Syntax Description

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

## Defaults

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 <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

## 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
	<b>ip igmp v3lite</b>	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
	<b>ip urd</b>	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	
<b>vrf</b>	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name assigned to the VRF.

**Defaults** 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 <b>vrf</b> keyword and <i>vrf-name</i> argument were added.
	12.2(13)T	The <b>vrf</b> keyword and <i>vrf-name</i> argument were added.

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

**Examples** The following example disables 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
	<b>ip pim state-refresh origination-interval</b>	Configures the origination of and the interval for the PIM dense mode state refresh control messages on a PIM router.
	<b>show ip pim interface</b>	Displays information about interfaces configured for PIM.
	<b>show ip pim neighbor</b>	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**

<b>Syntax Description</b>	<i>interval</i>	(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.
---------------------------	-----------------	---

<b>Defaults</b>	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 process and forward PIM dense mode state refresh control messages.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(5)T	This command was introduced.

<b>Usage Guidelines</b>	<p>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.</p> <p>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.</p>
-------------------------	--

<b>Examples</b>	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
```

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

## 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

<i>number</i>	Maximum number of VCs that PIM can open. The default is 200 VCs. The range is from 1 to 65535.
---------------	--

### Defaults

200 VCs per ATM interface or subinterface

### Command Modes

Interface configuration

### Command History

Release	Modification
11.3	This command was introduced.

### Examples

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

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

### Related Commands

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

**Defaults** Version 2

**Command Modes** Interface configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

**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
```

# ip rgmp

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

**ip rgmp**

**no ip rgmp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

RGMP is not enabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(10)S	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

## Usage Guidelines

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

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

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

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

The following features must be enabled on your switch:

- IP multicast
- IGMP snooping

## Examples

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

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

Related Commands	Command	Description
	<b>debug ip rgmp</b>	Logs debug messages sent by an RGMP-enabled router.
	<b>show ip igmp interface</b>	Displays multicast-related information about an interface.

# ip sap cache-timeout

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

**ip sap cache-timeout** *minutes*

**no ip sap cache-timeout**

## Syntax Description

<i>minutes</i>	Time (in minutes) that a SAP cache entry is active in the cache.
----------------	--

## Defaults

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

## Command Modes

Global configuration

## Command History

Release	Modification
11.2	The <b>ip sdr cache-timeout</b> command was introduced.
12.2	The <b>ip sdr cache-timeout</b> command was replaced by the <b>ip sap cache-timeout</b> command.

## Usage Guidelines

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

## Examples

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

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

## Related Commands

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

# ip sap listen

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

**ip sap listen**

**no ip sap listen**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The command is disabled.

**Command Modes** Interface configuration

## Command History

Release	Modification
11.1	The <b>ip sdr listen</b> command was introduced.
12.2	The <b>ip sdr listen</b> command was replaced by the <b>ip sap listen</b> command.

## Usage Guidelines

Cisco IOS software can receive and store Session Description Protocol (SDP) and Session Announcement Protocol (SAP) session announcements.

SAP is a protocol used to announce multicast multimedia conferences and other multicast sessions, and it is used to communicate session setup information to prospective participants. A SAP announcer periodically sends an announcement packet to a well-known multicast address and port. The announcement is sent via multicast with the same scope as the session it is announcing to ensure that the recipients of the announcement can also be recipients of the session the announcement describes. SAP should be used for sessions of public interest where participants are not known in advance.

When the **ip sap listen** command is configured on an interface, the well-known session directory groups on that interface can receive and store session announcements. Each announcer listens to other announcements in order to determine the total number of sessions being announced on a particular group, and the interfaces are put into the outgoing interface list for the IP SAP group. The announcements can be displayed with the **show ip sap** command. The **ip multicast rate-limit** command uses stored session announcements. To configure the period of time after which received announcements will expire, use the **ip sap cache-timeout** command.

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

**Examples**

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

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

**Related Commands**

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

## ip sdr cache-timeout

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

# ip sdr listen

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

# ip urd

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

**ip urd [proxy]**

**no ip urd [proxy]**

## Syntax Description

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

## Defaults

The command is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.1(3)T	This command was introduced.

## Usage Guidelines

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

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

## Examples

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

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip pim ssm</b>	Defines the SSM range of IP multicast addresses.