ip multicast cache-headers

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

ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]

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

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rtp	(Optional) Caches Real-Time Transport Protocol (RTP) headers.

Defaults

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1	The **rtp** keyword was added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

You can store IP multicast packet headers in a cache and then display them to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- User Datagram Protocol (UDP) port numbers
- Packet length

Note This command allocates a circular buffer of approximately 32 KB. Do not configure this command if you are low on memory.

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

Examples

The following example allocates a buffer to store IP multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache header buffer.
show ip mpacket quality	Displays an RTP data quality based on packets captured in the IP multicast cache header buffer.

ip multicast heartbeat

To monitor the health of multicast delivery and be alerted when the delivery fails to meet certain parameters, use the **ip multicast heartbeat** command in global configuration mode. To disable the heartbeat, use the **no** form of the command.

ip multicast heartbeat *group-address minimum-number window-size interval*

no ip multicast heartbeat *group-address minimum-number window-size interval*

Syntax Description

group-address	A multicast group address (Class D address, from 224.0.0.0 to 239.255.255.255)
minimum-number	Minimal number of intervals where the heartbeats must be seen. The number must be less than or equal to the window size.
window-size	Number of intervals to monitor for the heartbeat.
interval	Number of seconds interval to receive packet. Value must be a multiple of 10.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The subject group is joined at the subject interface so that multicast data for the subject group will be attracted toward the subject router.

The router monitors multicast packets destined to the group address at the *interval* value. This is a binary decision. That is, the number of packets seen in this period is not as important as whether any packet for the group is seen.

If multicast packets were observed in less than the *minimum-number* value out of the last *window-size* value intervals, a Simple Network Management Protocol (SNMP) trap would be sent from this router to a network management station to indicate a loss of heartbeat exception. This trap will be defined in CISCO-IPMROUTE-MIB.my.

The *interval* value must be a multiple of 10. In multicast distributed switching (MDS), statistics from the Versatile Interface Processor (in the Route Switch Processor) or the Label Controller (in the Gigabit Switch Router) are passed to the routing processor once every 10 seconds. Monitoring packets not in intervals of multiple of 10 seconds may lead to incorrect decisions.

This command does not create any multicast routing entries that are necessary for the monitoring of the heartbeat packets. These entries can be created by either the downstream members of the group, or with the **ip pim join-group** or **ip pim static-group** command. If a multicast routing entry corresponding to a group address expires due to lack of interest from the downstream members, the monitoring for the subject group would not work; that is, no more SNMP traps would be sent.

Examples

The following is an example configuration of the **ip multicast heartbeat** command:

```
snmp-server enable traps ipmulticast-heartbeat
ip multicast heartbeat 224.0.1.53 1 1 10
```

In this example, multicast packets forwarded through this router to group address 224.0.1.53 will be monitored. If no packet for this group is received in a 10-second interval, an SNMP trap will be sent to a designated SNMP management station.

Note It may take about 20 seconds of losing the multicast feed before the SNMP trap is sent.

Related Commands

Command	Description
debug ip mhbeat	Monitors the action of the heartbeat trap.
snmp-server enable traps	Enables the router to send SNMP traps.

ip multicast helper-map

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

ip multicast helper-map {*group-address broadcast-address* | **broadcast** *multicast-address*} *access-list*

no ip multicast helper-map {*group-address broadcast-address* | **broadcast** *multicast-address*} *access-list*

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

ip multicast helper-map broadcast *multicast-address access-list* [**ttl** *reset-value*]

no ip multicast helper-map broadcast *multicast-address access-list*

Syntax Description

group-address	Multicast group address of traffic to be converted to broadcast traffic. Use this value with the *broadcast-address* value.
broadcast-address	Address to which broadcast traffic is sent. Use this value with the *group-address* value.
broadcast	Specifies the traffic is being converted from broadcast to multicast. Use this keyword with the *multicast-address* value.
multicast-address	IP multicast address to which the converted traffic is directed. Use this value with the **broadcast** keyword.
access-list	IP extended access list number or name that controls which broadcast packets are translated, based on the User Datagram Protocol (UDP) port number.
ttl *reset-value*	(Optional) Translates packets with a time-to-live (TTL) of 1 and resets the TTL to the value specified for *the reset-value* argument. Valid values are from 1 to 50.

Command Default

No conversion between broadcast and multicast occurs.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When a multicast-capable internetwork is between two broadcast-only internetworks, you can convert broadcast traffic to multicast at the first hop router, and convert it back to broadcast at the last hop router before delivering the packets to the broadcast clients. However, broadcast packets with the IP source address of 0.0.0.0 (such as a Dynamic Host Configuration Protocol [DHCP] request) will not be translated to any multicast group.

Thus, you can take advantage of the multicast capability of the intermediate multicast internetwork. This feature prevents unnecessary replication at the intermediate routers and allows multicast fast switching in the multicast internetwork.

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

Note On Catalyst 6500 series switches and Cisco 7600 series routers, broadcast packets with a TTL of 1 are not translated by the **ip multicast helper-map** command unless you use the **ttl** keyword with the command.

Examples

The following example illustrates how a helper address on two routers converts traffic from broadcast to multicast and back to broadcast.

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

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

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

First Hop Router Configuration

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

Last Hop Router Configuration

```
interface ethernet 1
 ip address 126.1.26.1 255.255.255.0
 ip pim sparse-mode
 ip multicast helper-map 239.254.2.5 126.1.28.255 105

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

Related Commands

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

ip multicast multipath

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

ip multicast [**vrf** *vrf-name*] **multipath**

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

Syntax Description

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

Defaults

By default, if multiple equal-cost paths exist, multicast traffic will not be load split across these paths.

Command Modes

Global configuration

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

If the **ip multicast multipath** command is configured and multiple equal-cost paths exist, load splitting will occur across the equal-cost paths for multicast traffic from different sources to the same multicast group, but not for traffic from the same source to different multicast groups. Because this command changes the way a Reverse Path Forwarding (RPF) neighbor is selected, it must be configured consistently on all routers in a redundant topology to avoid looping.

Examples

The following example shows how to configure the **ip multicast multipath** command:

```
ip multicast multipath
```

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

ip multicast rate-limit

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

ip multicast rate-limit {**in** | **out**} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip multicast ttl-threshold

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

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold *ttl-value*

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

ip multicast use-functional

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

ip multicast use-functional

no ip multicast use-functional

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command is accepted only on a Token Ring interface.

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

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

Examples

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

```
interface token 0
 ip address 1.1.1.1 255.255.255.0
 ip pim dense-mode
 ip multicast use-functional
```

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

Syntax Description

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.
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 the extended access list number or name.
route-map *map-name*	(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 **sparse-dense-mode** keyword was added.
12.0 S	The following keywords and arguments were added: • **proxy-register** • **list** *access-list* • **route-map** *map-name*

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
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
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 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

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
list *access-list*	Defines the extended access list number or name.
route-map *map-name*	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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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

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.

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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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
```

Related Commands

Command	Description
access-list (IP standard)	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

Disabled

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

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(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 **vrf** keyword and *vrf-name* 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 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.
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 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 in this chapter 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

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

When this command is configured on an interface, no 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 only sets up 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 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

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 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).
hash-mask-length	(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.
priority	(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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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
ip pim border	Configures the interface to be the PIM domain border.
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	Configures the router to be an RP-mapping agent.
show ip pim bsr	Displays the BSR information.
show ip pim rp	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*

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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

When a DR is elected, 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 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 [*pps*]

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.

Defaults

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 Virtual Circuits" 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
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.

Defaults

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
atm multipoint-signalling	Enables point-to-multipoint signalling to the ATM switch.
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.

Defaults

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
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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
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
```

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 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 *seconds*

no ip pim query-interval [*seconds*]

Syntax Description

seconds	Interval, in seconds, at which periodic PIM router query messages are sent. It can be a number from 1 to 65535. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example changes the PIM router query message interval to 45 seconds:

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

Related Commands

Command	Description
ip igmp query-interval	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

vrf *vrf-name*	Specifies that the rate-limit for register messages be applied to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rate	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 **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.
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
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** *interface-type interface-number*

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.

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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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 a particular group, 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 rp-address *rp-address* [*access-list*] [**override**] [**bidir**]

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

Syntax Description

rp-address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.
access-list	(Optional) Number or name of an access list that defines for which multicast groups the RP should be used.
override	(Optional) Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by Auto-RP.
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.

Defaults

No PIM RPs are preconfigured.

Command Modes

Global configuration

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.

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 via 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 statistically 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 sets 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 sets 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
access-list (IP standard)	Defines a standard IP access list.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the bootstrap router.
ip pim send-rp-announce	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

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rp-list *access-list*	Specifies the number or name of a standard access list of RP addresses that are allowable for the group ranges supplied in the **group-list** *access-list* combination.
group-list *access-list*	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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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*] [**interface** *seconds*] [**priority** *value*]

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

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	The IP address associated with this interface type and number is advertised as a candidate 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 must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
priority *value*	(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 **bidir** keyword was added.

Release	Modification
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.

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
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* **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]

no ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-type interface-number* **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]

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.
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 option, 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: • **interval** *seconds* • **bidir**
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.

Usage Guidelines

Use this command in the router 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
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 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** [*interface-type interface-number*] **scope** *ttl-value*

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	(Optional) Interface type and number that is used to define the RP mapping agent address.
scope *ttl-value*	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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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** {*kbps* | **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps* | **infinity**} [**group-list** *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.
kbps	Traffic rate (in kbps).
infinity	Causes all sources for the specified group to use the shared tree.
group-list *access-list*	(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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.

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 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** {**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.

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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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
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.

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 **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* 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
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.

Defaults

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.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

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.

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 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.

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
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.
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.

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 1.1.1.1 255.0.0.0
 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 enabling RGMP, the following features must be enabled on your router:

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

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

The following features must be enabled on your switch:

- IP multicast
- IGMP snooping

Examples

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

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

Related Commands

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

ip rtp compression-connections

To specify the total number of Real-Time Transport Protocol (RTP) header compression connections that can exist on an interface, use the **ip rtp compression-connections** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip rtp compression-connections *number*

no ip rtp compression-connections

Syntax Description

number	Number of RTP header compression connections the cache supports, in the range from 3 to 1000. The default is 32 connections (16 calls).

Defaults

32 connections

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(7)T	For PPP and High-Level Data Link Control (HDLC) encapsulation, the maximum number of connections increased from 256 to 1000. For Frame Relay encapsulation, the maximum number of connections increased to 256. The maximum value for Frame Relay is fixed, not configurable.

Examples

The following example changes the number of RTP header compression connections supported to 150:

```
interface serial 0
 encapsulation ppp
 ip rtp header-compression
 ip rtp compression-connections 150
```

Related Commands

Command	Description
frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip rtp header-compression	Enables RTP header compression per DLCI.
ip rtp header-compression	Enables RTP header compression.
ip tcp header-compression	Enables TCP header compression.
show ip rtp header-compression	Displays RTP header compression statistics.

ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression, use the **ip rtp header-compression** command in interface configuration mode. To disable RTP header compression, use the **no** form of this command.

ip rtp header-compression [**passive**]

no ip rtp header-compression [**passive**]

Syntax Description

passive	(Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you use this command without the **passive** keyword, the software compresses all RTP traffic.

You can compress IP/User Datagram Protocol (UDP)/RTP headers to reduce the size of your packets. Compressing headers is especially useful for RTP, because RTP payload size can be as small as 20 bytes, and the uncompressed header is 40 bytes.

RTP header compression is supported on serial lines using Frame Relay, High-Level Data Link Control (HDLC), or PPP encapsulation. You must enable compression on both ends of a serial connection.

This command can compress unicast or multicast RTP packets, and hence multicast backbone (MBONE) traffic can also be compressed over slow links. The compression scheme is beneficial only when you have small payload sizes, as in audio traffic.

Examples

The following example enables RTP header compression on serial interface 0 and limits the number of RTP header compression connections to 10:

```
interface serial 0
 encapsulation ppp
 ip rtp header-compression
 ip rtp compression-connections 10
```

Related Commands

Command	Description
clear ip rtp header-compression	Clears RTP header compression structures and statistics.
ip rtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
show ip rtp header-compression	Displays RTP header compression statistics.

ip sap cache-timeout

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

ip sap cache-timeout *minutes*

no ip sap cache-timeout

Syntax Description

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

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 **ip sdr cache-timeout** command was introduced.
12.2	The **ip sdr cache-timeout** command was replaced by the **ip sap cache-timeout** 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
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
show ip sap	Displays the SAP cache.